Abstract. Today's computing infrastructure is built atop layers of legacy C code, often insecure, poorly understood, and/or difficult to maintain. These foundations may be shored up with dynamic security enforcement, which spares legacy code owners from having to modify their code. Tagged C is a C variant with a built-in *tag-based reference monitor* for use in expressing a variety of dynamic security policies and enforcing them with compiler and hardware support.

Tagged C is comprehensive in the policies that it can support. In this paper we will discuss *memory safety*, *compartmentalization*, and *secure information flow* (SIF) policies. It is flexible in covering the tradeoff between conservative policies that may halt too many programs and more permissive ones. And as a source language, it should be more accessible to C programmers than existing assembly-level tag-based reference monitors.

Flexible Runtime Security Enforcement with Tagged C

Sean Anderson, Allison Naaktgeboren, and Andrew Tolmach

Portland State University

1 Introduction

Many essential technologies rely on new and old C code. Operating systems (Linux, Windows, OSX, BSD), databases (Oracle, sqlite3), the internet & web (Apache, NGNIX, NetBSD, Cisco IOS), the Internet of Things (IoT), and the embedded devices that run our homes and hospitals are built in and on C [9]. C is not a relic; more than a third of professional programmers report active developing in C today [10]. The safety of public and private systems we depend on every day in turn depends on the security of their underlying C codebases. Insecurity might take the form of undefined behavior such as memory errors, of logic errors such as sql injection or other input-sanitization flaws, or of larger-scale architectural flaws that over-provision components of the system with privilege.

The last line of defense against unknown or unfixable vulnerabilities is dynamic enforcement at runtime. To this end, we introduce Tagged C: a general-purpose dynamic tag-based enforcement language that allows developers to define flexible security policies on top of their existing C codebases, from defining memory UB to specifying detailed information flow policies.

[APT: ... the para makes it sound like we are only interested in C language errors. But bugs in the programmer's logic are at least as important for the properties we are trying to enforce!] AN: I thought the focus was on C UB limiting and thats kinda C specific? Are there logic errors in any of our example sections? [SNA: SQL injection and information leaks are logic errors]

A tag-based reference monitor associates a metadata tag with the data in the underlying system, and throughout execution it updates these tags according to a set a predefined rules, or halts if the program would violate a rule, replacing a security violation with failstop behavior. By attaching such a monitor to the C language, we allow a user to apply whatever security policy meets their needs, tuned if necessary so that non-standard but benign code can still run, while actually dangerous activity is halted.

[SNA: Explicitly call out that we can change things without recompilation]

Tagged C consists of an underlying semantics that establishes the baseline concrete behavior of programs with no policies, and a set of *control points* at which the semantics consult a user defined set of *tag rules*. Our underlying semantics are built on the CompCert C semantics, the C semantics formalized along with the CompCert verified compiler [8]. We provide a reference interpreter also based on that of CompCert. [SNA: I feel some need to justify this, but I'm not sure what justification is appropriate.]

Why C-Level? Tag-based enforcement in general has a significant body of work at the assembly level, especially PIPE (Programmable Interlocks for Policy Enforcement) []. However, even at the assembly-level these systems need the compiler to be in the trusted computing base (TCB), as many policies require knowledge of source-level constructs, even ones that do not depend on detailed knowledge of the program's behavior [cite Nick and Andre; anyone else?]. Moving policy-definition to the source level therefore does not expand the TCB and allows C developers to reason about policies in terms of the language that they program in regularly.

Contributions We offer the following contributions:

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

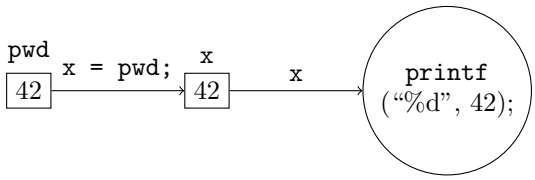
In the next section, we give a high-level introduction of metadata-tagging: how it works, and how that can improve security. Then in section 3, we briefly discuss the language as a whole, before moving into policies in section 4. Finally, in **??** we discuss the degree to which the design meets our goals of flexibility and applicability to realistic security concerns.

2 What is Metadata Tagging?

[APT: I think this example works pretty well, but diagrams are not clear yet.]

Consider a very simple security requirement: "do not `printf` the password." For simplicity, we will suppose that `pwd` is an integer in this case.

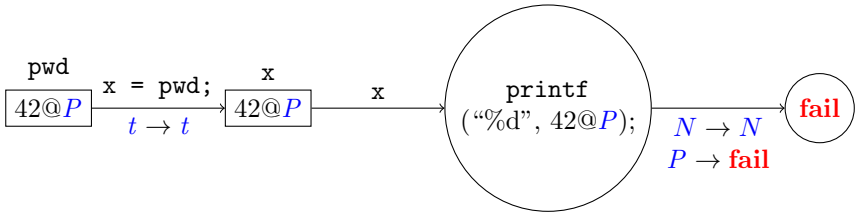
```
void main(int pwd) {
  int x = pwd;
  printf("%d", x);
}
```



[APT: Not clear what the labels on edges mean. (And why is there a font change in the figure?)]

We need a way to dynamically track the confidential status of `pwd` as it moves through the variable `x` and is then passed to `printf`. We can do so by associating metadata with the value; namely, that it originates in `pwd`. We will write this "tagged" value 42@P, with the @ symbol denoting a value tagged with metadata. All other values will be tagged N, for "not `pwd`." Then when we

copy `pwd` into `x`, it will bring its tag with it unchanged, as represented by the pattern $t \to t$ under the arrow. When we call `printf`, we must check that the tag is N, and if it is P, we would like to failstop rather than permit the call.

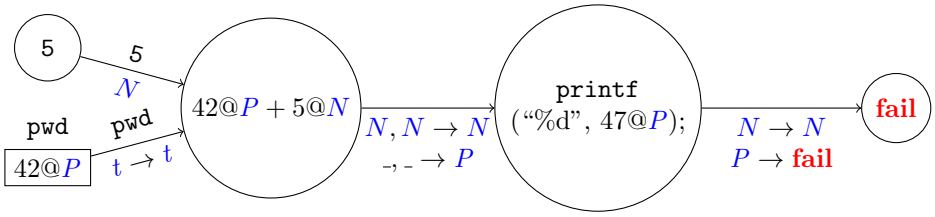


[APT: Arrow to "fail" is confusing. We should only go there is tag on x is P. And it is unclear that the N and P on the arrow label are attached to the printed value.]

The points at which the tags are checked and either propagated or updated are termed *control points*, and the particular set of rules that are applied to tags at each control point is a *tag rule*. Collectively, the tag rules form a *policy*.

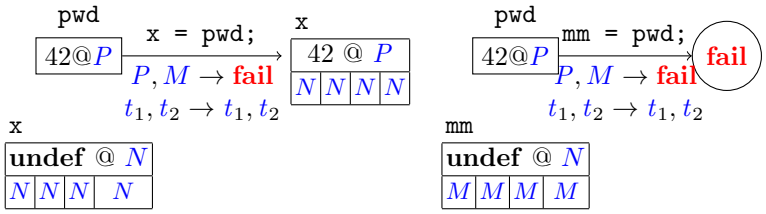
If our goal is to prevent `pwd` from being leaked, our policy should also prevent values derived from `pwd` from leaking. This means that if we add `pwd` to a constant, we still keep the result tagged P—otherwise, someone watching our output could deduce P by subtraction.

```
void main(int pwd) {
  printf(pwd+5);
}
```



Function calls aren't the only means of leaking data, however. We might additionally want to prevent `pwd` from leaking by being written mmapped memory. Supposing the `mm` is such a location, we would separately tag the location itself (not just the value in the location) to designate it as such. We'll call that tag M. [TODO: the diagrams for this are pretty rough.]

```
void main(int pwd) {
  int x = pwd;
  mm = pwd;
}
```



Finally, we may be concerned with implicit leaks of `pwd`, such as this one:

```
void main(int pwd) {
  for (int i; i<pwd; i++) {
    printf(i);
  }
}
```

This will give away the exact value of `pwd`! In order to prevent this, we must keep track of when we are inside of a loop or conditional that depends on `pwd`. To this end, we carry an additional tag associated with the global state. This is called the PC Tag, written $\mathcal{P}$. In examples that show states we will note it alongside the statement under focus.

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. [APT: Oops. What's PIPE?] 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.

[APT: Not clear this belongs in the intro.] 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.

3 The Language

Tagged C uses the full syntax of CompCert C [8] with minimal modification (fig. 6). There are two notable syntactical differences in the language, relative to CompCert C: conditionals and loops take an optional *join point* label, and parenthetical expressions an optional "context tag."

Our semantics are a small-step reduction semantics which differ from CompCert C's in two key respects. These are given in full in the appendix. First,

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 4.

Second, 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.

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.

Notations 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, $\mathcal{P}$ 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 6), statements by s, and continuations by k. The continuations are defined in appendix B, and step rules in appendix D.

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" $\overline{lt}$.

A memory is an array of bytes, where each byte is part of an atom. Each byte is also associated with a "location tag" lt. When a contiguous region of s bytes starting at location l comprise an atom $v@vt$, and their locations tags comprise the list $\overline{lt}$, we write $m[l]_s = v@vt@\overline{lt}$. Likewise, $m[l \ldots l+s \mapsto v@vt@\overline{lt}]_s$ denotes storing that many bytes. Visually, we will represent whole atoms in memory as condensed boxes, with their location tags separate. For example, a four-byte aligned address:

l

$v@vt$			
lt_1	lt_2	lt_3	lt_4

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

the state that produced the failure. [Allison: to whatever degree you've figured out what is useful here by publication-time, we can tune this to be more specific.]

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

4 Tags and Policies

Name	Inputs	Outputs	Control Points
GlobalT	$id \in ident, s \in \mathbb{N}$	$pt, vt, \overline{lt}$	Program initialization
FieldT	pt, id	pt'	Field Access
LoadT	$\mathcal{P}, pt, vt, \overline{lt}$	vt'	ValOf, AssignOp, PostIncr
StoreT	$\mathcal{P}, pt, vt_1, vt_2, \overline{lt}$	$\mathcal{P}', vt', \overline{lt}'$	Assign
ConstT		vt	Const, PostIncr
UnopT	$\odot, \mathcal{P}, vt$	vt	Unary Operation
BinopT	$\oplus, \mathcal{P}, vt_1, vt_2$	vt'	Binary Operation
MallocT	$\mathcal{P}, vt$	$\mathcal{P}', pt, \boxed{vt, \overline{lt}}$	Call to `malloc`
FreeT	$\mathcal{P}, vt$	$\mathcal{P}', pt, \boxed{vt, \overline{lt}}$	Call to `free`
PICastT	$\mathcal{P}, pt, \boxed{vt, \overline{lt}}$	vt	Cast from pointer to scalar
IPCastT	$\mathcal{P}, vt_1, \boxed{vt_2, \overline{lt}}$	pt	Cast from scalar to pointer
PPCastT	$\mathcal{P}, pt, \boxed{vt, \overline{lt}}$	pt'	Cast between pointers
IICastT	$\mathcal{P}, vt_1$	pt	Cast between scalars
ExprSplitT	$\mathcal{P}, vt$	$\mathcal{P}'$	Control-flow split points in expressions
ExprJoinT	$\mathcal{P}, \mathcal{P}', vt$	$\mathcal{P}'', vt'$	Parenthetical expressions
SplitT	$\mathcal{P}, vt, \boxed{L}$	$\mathcal{P}'$	Split points (**??**)
LabelT	$\mathcal{P}, L$	$\mathcal{P}'$	Label
CallT	$\mathcal{P}, f, f'$	$\mathcal{P}'$	Call
ExtCallT	$\mathcal{P}, f, f', \overline{vt}$	$\mathcal{P}'$	External Call
LocalT	$\mathcal{P}, x \in ident, s \in \mathbb{N}$	$pt, vt, \overline{lt}$	Call
ArgT	$\mathcal{P}, vt, f, x, s$	$\mathcal{P}', pt, vt', \overline{lt}$	Call
RetT	$\mathcal{P}_{CLE}, \mathcal{P}_{CLR}, vt, f$	$\mathcal{P}', vt'$	Return
DeallocT	$\mathcal{P}, id \in ident, s \in \mathbb{N}$	$vt, \overline{lt}$	Return

Tagged C can enforce a wide range of policies, as follows. A policy consists of a tag type τ, a default tag inhabiting that type, and an instantiation of each tag rule identified in section 4.

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 charac-

terization 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. [4] 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 the following constructions and identify them as follows:

- Function identifiers, $FN(f)$
- Function arguments, $AN(f, x)$
- Global variables, $GN(x)$
- Labels, $LN(L)$
- Types, $TN(ty)$

4.1 Basic Memory Safety

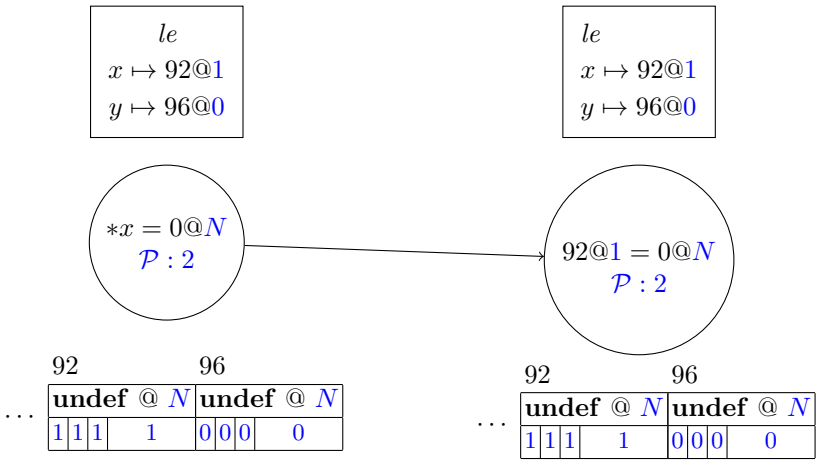
Let's begin by walking through a common type of policy: memory safety. Variations of memory safety have been enforced in PIPE at the assembly level already, but what does it look like to enforce it at the source level? Consider some example code:

```
void main() {
  int[1] x;
  int[1] y;
  *x = 0;
  *(x+1) = 0;
}
```

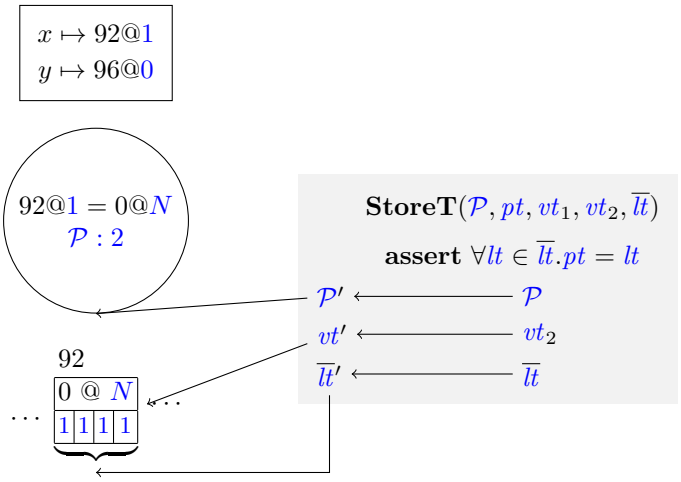
The above code is undefined behavior in C, because it writes to the address one past the end of the array pointed to by `x`. Since `x` and `y` are given adjacent concrete addresses, when the program writes to the address of `x+1`, it is writing to the address of `y`. For our example, we'll assume that the stack grows downward from address 100.

We can prevent situations like this using a *memory safety* policy, as follows. We assign to each object in memory a unique "color" when it is allocated—in this case, on entry to the function `main`.

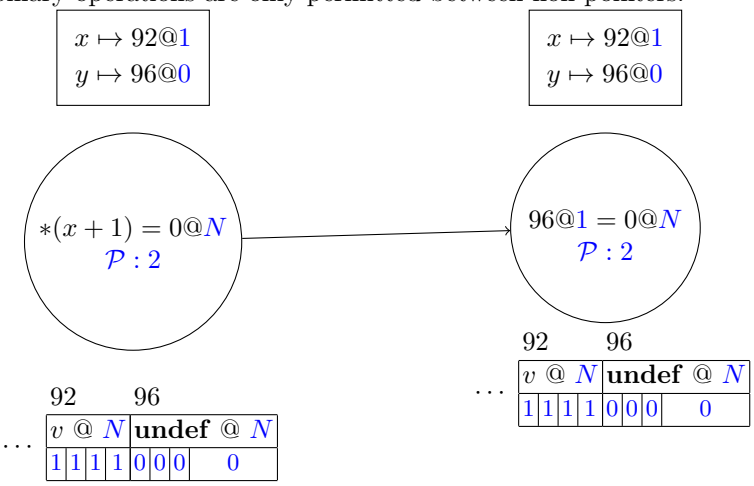
Our set of tags consists of N, for non-pointers, and pointer "colors" $c \in \mathbb{N}$. The PC Tag ($\mathcal{P}$) tracks the next color to allocate, so it's initialized to 0, and everything else is N. N is the default for constants.



Next, the program stores a 0 to address 1000. The constant 0 takes on the default tag, I. The policy needs to check that this store is valid, in addition to determining the tags on the value that is stored. This check is performed by comparing the tag on the pointer to the tags on memory—each byte being written, in case the pointer is misaligned. Then the tag on the value being stored is propagated with it into memory, unchanged. [TODO: arrows aren't pointing to quite the right places right now, but one can imagine.]



Next, on the last line, we add 1 to `x`, which invokes the **BinopT** tag rule to combine the tags on the arguments. **BinopT** takes as argument the operation $\oplus$. In memory safety terms, we can add a pointer to a non-pointer in either order, and we can subtract a non-pointer from a pointer (but not the reverse), to yield a pointer to the same object. We can subtract two pointers to the same object from one another to yield a non-pointer, the offset between them. All other binary operations are only permitted between non-pointers.



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

$\mathcal{P}' \longleftarrow \mathcal{P}$

$$vt' \longleftarrow \begin{cases} c & \text{when } (\oplus,\ vt_1,\ vt_2) \text{ is } +, c, N \mid +, N, c \mid -, c, N \\ N & \text{is } -, c, c \mid \_, N, N \\ \textbf{fail} & \text{is otherwise} \end{cases}$$

So, when we try to write through the address 96@1, we compare its tag to that of the memory locations, which are tagged 0. Therefore the policy must failstop on the store.

4.2 PVI Memory Safety

The simple memory safety policy described above is too restrictive to run many real-world C programs, because they contain undefined behavior that is nevertheless part of the "de facto standard" [**?**]. These low-level idioms are one reason that we might settle for isolating risky code in a compartment instead of enforcing full memory safety.

Memarian et al. [**?**] propose two memory models that aim to capture this de facto standard, support the common low-level idioms, yet still place sufficient restrictions on programs that it remains sound to use alias analysis in optimizations. The first of these is *PVI* (provenanace via integer), in which pointers remain valid when they are cast to integers, subjected to the full range of arithmetic operations, and cast back. Memarian et al. do not propose to enforce PVI, merely to use it as an alternative to the C standard. But its relative permissiveness makes it a great target for enforcement in Tagged C! Their second memory model, *PNVI* (provenance not via integer), is even more permissive. We can also enforce it in Tagged C, though its security value is questionable, and we will not describe it in this paper.

[TODO: For example, garbage collectors use low order bits to mark pointers as in the Cheney algorithm.]

PVI Definitions Since PVI is a more realistic policy than the basic memory safety described above, we will go into some details elided there. First of all, the distinction between heap-allocated memory, stack objects, and global variables. The latter are tagged based on their identifiers, while heap- and stack-objects are tagged dynamically using unique colors.

$$\begin{array}{rl} \tau ::= & \mathit{glob}\ \mathit{id} \\ & \mathit{dyn}\ C \end{array} \qquad \begin{array}{r} \mathit{id} \in \mathit{ident} \\ C \in \mathbb{N} \end{array}$$

When initializing program memory, before any execution, each global *id* has its memory locations and its pointer in the global environment tagged with *glob id*, using the **GlobalT** tag rule.

$$\begin{array}{rl} & \textbf{GlobalT}(\mathit{id}, s) \\ \boldsymbol{pt} \longleftarrow & \mathit{glob}\ \mathit{id} \\ \boldsymbol{vt} \longleftarrow & N \\ \overline{\boldsymbol{lt}} \longleftarrow & [\mathit{glob}\ \mathit{id} \mid 0 \leq i < s] \end{array}$$

In our previous memory safety example, we began with the active stack frame already allocated. When it is allocated at runtime, its tags are initialize by the **LocalT** rule. Stack-allocated locals and heap-allocated objects both

The tag rules for allocating memory in the heap and in the stack should look familiar.

$$\textbf{LocalT}(\mathcal{P}, x, s)$$

$$\begin{aligned} \boldsymbol{pt} &\longleftarrow \mathit{dyn}\ \mathcal{P} \\ \boxed{\boldsymbol{vt}} &\longleftarrow N \\ \boxed{\overline{\boldsymbol{lt}}} &\longleftarrow [\mathit{dyn}\ \mathcal{P}] \\ \boldsymbol{\mathcal{P}'} &\longleftarrow \mathcal{P} + 1 \end{aligned}$$

$$\textbf{MallocT}(\mathcal{P}, vt)$$

$$\begin{aligned} \boldsymbol{pt} &\longleftarrow \mathit{dyn}\ \mathcal{P} \\ \boxed{\boldsymbol{vt}} &\longleftarrow N \\ \boxed{\overline{\boldsymbol{lt}}} &\longleftarrow [\mathit{dyn}\ \mathcal{P}] \\ \boldsymbol{\mathcal{P}'} &\longleftarrow \mathcal{P} + 1 \end{aligned}$$

Color Checking As in the basic policy, 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.

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

$$\begin{aligned} &\textbf{assert}\ \forall lt \in \overline{lt}.pt = lt \\ vt' &\longleftarrow vt \end{aligned}$$

$$\textbf{StoreT}(\mathcal{P}, pt, vt_1, vt_2, \overline{lt})$$

$$\begin{aligned} &\textbf{assert}\ \forall lt \in \overline{lt}.pt = lt \\ \mathcal{P}' &\longleftarrow \mathcal{P} \\ vt' &\longleftarrow vt_2 \\ \overline{lt}' &\longleftarrow \overline{lt} \end{aligned}$$

Color Propagation In our example memory safety policy, we placed significant restrictions on the ways that pointer-tagged values could be subject to integer operations. In PVI, this is not the case: all unary operations maintain the tag on their input, and all binary operations where exactly one argument is tagged as a pointer propagate that tag to their result. Performing an operation with two pointer-tagged values sets the tag on the result to N. It can still be used as an integer, but if cast back to a pointer it will be invalid.

$$\textbf{UnopT}(\odot, \mathcal{P}, vt)$$

$$\begin{aligned} \mathcal{P}' &\longleftarrow \mathcal{P} \\ vt' &\longleftarrow vt \end{aligned}$$

$$\textbf{BinopT}(\oplus, \mathcal{P}, vt_1, vt_2)$$

$$\begin{aligned} \mathcal{P}' &\longleftarrow \mathcal{P} \\ vt' &\longleftarrow \begin{cases} t & \text{when } (\oplus,\ vt_1,\ vt_2) \text{ is } (\_, t, N) \\ t & \text{is } (\_, N, t) \\ N & \text{is } -, \mathit{dyn}\ n_1, \mathit{dyn}\ n_2 \\ \textbf{fail} & \text{is otherwise} \end{cases} \end{aligned}$$

4.3 Compartmentalization

In a perfect world, all C programs would be memory safe. But it is unfortunately common for a codebase to contain undefined behavior that will not be fixed, including memory undefined behavior. This may occur because developers intentionally use low-level idioms that are UB [**?**]. Or the cost and potential risk of regressions may make it undesirable to fix bugs in older code, as opposed to code under active development that is held to a higher standard [3].

A compartmentalization policy isolates potentially risky code, such as code with known UB, from safety-critical code, minimizing the damage that can be done if a vulnerability is exploited. This is a very common form of protection that can be implemented at many levels. It is often built into a system's fundamental design, like a web browser sandbox untrusted javascript. But for our use-case, we consider a compartmentalization scheme being added to the system after the fact.

[TODO: a few words about least privilege, the other main compartmentalization use.]

Let's assume that we have a set of compartment identifiers, ranged over by C, and a mapping from function identifiers to compartments, $comp(f)$. This mapping must be provided by a security engineer.

Coarse-grained Protection The core of a compartmentalization scheme is once again memory protection. For the simplest version, we will enforce that memory allocated by a function is only accessible by functions that share its compartment. To do that, we need to keep track of which compartment we're in, using the PC Tag.

Calls and returns each take two steps: first to an intermediate call or return state, and then to the normal execution state, as shown in fig. 1 with some function f calling f'. Three of these steps feature control points. In the initial call step, **CallT** uses the name-tags of the caller and callee to update the PC Tag. Then, in the step from the call state, we place the function arguments in the temp environment, tagging their values with the results of **ArgT**, and we allocate our stack locals, tagging their values and locations with the results of **LocalT**. And on return, **RetT** updates both the PC Tag and the tag on the returned value.

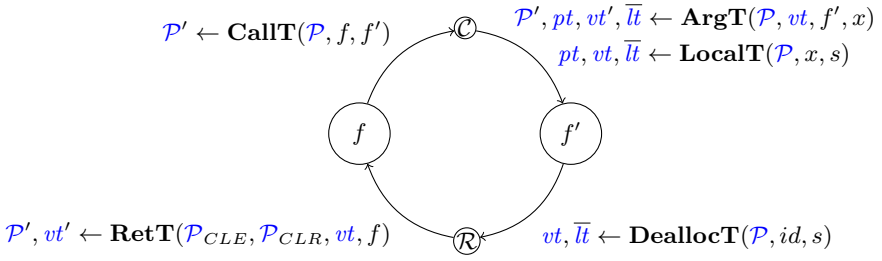


Fig. 1: Structure of a function call

In our compartmentalization policy, we define a tag to be a compartment identifier or the default N tag.

$$\tau ::= C | N$$

At any given time, the PC Tag carries the compartment of the active function. This is kept up to date by the **CallT** and **RetT** rules. Note that Tagged C automatically keeps track of the PC Tag at the time of a call, so that it can be used as a parameter in the return.

CallT$(\mathcal{P}, f, f')$

let $C := comp(f')$ *in*

$\mathcal{P}' \longleftarrow \mathcal{P}$

RetT$(\mathcal{P}_{CLE}, \mathcal{P}_{CLR}, vt, f)$

$\mathcal{P}' \longleftarrow \mathcal{P}_{CLR}$

$vt' \longleftarrow vt$

Now that we know which compartment we're in, we can make sure that its memory is protected. This will essentially work just like the basic memory safety policy, except that coarse-grained protection means that the "color" we assign to an allocation is the active compartment. And during a load or store, we compare the memory tags to the PC Tag, not the pointer.

MallocT$(\mathcal{P}, vt)$

$\mathcal{P}' \longleftarrow N$

$pt \longleftarrow N$

$vt \longleftarrow [\mathcal{P}]$

$lt \longleftarrow \mathcal{P}$

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

assert $\forall lt \in \overline{lt}.\mathcal{P} = lt$

$vt' \longleftarrow vt$

StoreT$(\mathcal{P}, pt, vt_1, vt_2, \overline{lt})$

assert $\forall lt \in \overline{lt}.lt = \mathcal{P}$

$\mathcal{P}' \longleftarrow \mathcal{P}$

$vt' \longleftarrow N$

$\overline{lt}' \longleftarrow \overline{lt}$

Sharing Memory The above policy works if our compartments only ever communicate by passing non-pointer values. In practice, this is far too restrictive! Many library functions take pointers and operate on memory shared with the caller. External libraries are effectively required for most software to function yet represent a threat. Isolating external libraries from critical code prevents vulnerabilities in the library from compromising critical code and deprives potential attackers of ROP gadgets and other tools if there is an exploit in the critical code.

To allow intentional sharing of memory across compartments, a more flexible policy is needed. Suppose for example the hostname needs to conform to an expected pattern, such as in an enterprise network, to differentiate between different classes of computers (employee, server, contractor, etc). The standard library, over in its own compartment, has helpful functions, provided the caller provides the buffers from which to set or get the hostname.

```
void configure_enterprise(char* intended_name) {
  int ret = 0;
  char curr_name = malloc(HOST_NAME_MAX + 1);
  ret = gethostname( &curr_name, HOST_NAME_MAX + 1 );
  if (! ret && curr_name != intended_name) { // !ret == (ret==0)
    ret = sethostname(intended_name), strlen(intended_name);
    ....
  }
```

```
  ....
}
```

[TODO: update this section for the new example code]

The literature contains two main approaches to this problem: *mandatory access control* and *capabilities*. The former explicitly enumerates the access rights of each compartment, while the latter turns passed pointers into unforgeable tokens of privilege, so that the act of passing one implicitly grants the recipient access.

We can handle a mix of allocations that will be passed and those that will not by creating a variant identifier for `malloc`, `malloc_share`. This identifier maps to the same address (i.e., it is still calling the same function) but its name tag differs and can therefore parameterize the tag rule. The source must have the malloc name changed for every allocation that might be shared. The annotation could be performed manually, or perhaps automatically using some form of escape analysis.

Mandatory Access Control Mandatory access control works by associating objects in memory with the compartments that are allowed to access them.

Memory Shared by Capability Mandatory access control requires the policy designer to identity every pair of object and compartment that it will be shared with. This may require too much analysis if objects are shared widely throughout the system. Conversely, it does not distinguish between accesses via a valid pointer and those that are the result of UB.

A capability model resolves both issues by treating shared pointers as tokens of privilege. If a compartment can obtain a shared pointer, we assume that it is allowed to access the associated memory. But the access must be performed using that pointer, ruling out other methods such as pointer forging.

$$
\begin{aligned}
\tau ::= & N \\
& \mathit{glob}\ C \\
& \mathit{dyn\_local}\ C \\
& \mathit{dyn\_share}\ c \\
& \mathit{comp}\ C\ c
\end{aligned}
$$

We define a predicate *cap* that holds when the target address is local to the active compartment or is shared and accessed through an appropriate capability.

4.4 Secure Information Flow

Memory safety and compartmentalization both either prevent or mitigate memory errors. But programs can be memory safe and still do insecure things! Consider the following code, in which we have some error-handling code that writes to a log. [TODO: more realistic example]

```
int checked_div(int a, int b) {
  if (a % b == 0) {
    return a / b;
  } else {
    fprintf(log, "%d should divide %d but doesn't\n", b, a);
    return 0;
  }
}

void main(int factor) {
  int key = read_and_parse(keyfile);
  int dividend = checked_div(key, factor);
  if (!dividend) { ... } else { ... }
}
```

The `checked_div` function sometimes writes its arguments to a log, which is reasonable enough, except when it's called with a key as an argument! Suddenly we have keys being written to an unexpected and probably unprotected file.

This is an instance of problematic information-flow. The solution is to implement a *secure information flow* (SIF) policy in Tagged C. SIF is a variant of *information flow control* (IFC) described in the venerable Denning and Denning [5]. At its simplest, if we classify inputs and outputs to the program into secure ("high") and public ("low") classifications, then the high inputs do not influence the low outputs. This generalizes to an arbitrary set of security classes, but out first example is concerned with just two: the value returned from `read_and_parse` and the output to the log. In our treatment of this example, we will describe a policy tailored to this particular set of security classes.

SIF Example Policy 1 Let's assume that `read_and_parse` is an *external* function—that is, we will not model its internal behavior, so we know nothing about the value it returns. We can therefore treat that value as an input, and track its influence through the system.

For this initial, simplified policy, we will assume that it is the only input that we care about, so we have four classes of tags. The default tag N represents values that are not tainted by the sensitive input, the tag $vtaint$ represents values that have been influenced by `read_and_parse`, and the tag $pc\ f\ \overline{L}$ carries a set of labels representing that the current control-flow of the program is tainted (we will discuss this in detail below.) Lastly, the tag vol marks the memory locations of *volatile* global variables. Volatile variables represent mmapped regions or memory that for other reasons is accessible outside the process.

Initially, the PC Tag is $pc\ f\ \emptyset$, and all values and memory locations are tagged N. The taint tags are introduced at the external call to `read_and_parse`. At the same time, all external calls must check that they aren't leaking a tainted value!

$$
\begin{array}{l}
\tau ::= N \\
\quad \mid \mathit{vtaint} \\
\quad \mid \mathit{pc}\ f\ \overline{L} \\
\quad \mid \mathit{vol}
\end{array}
\qquad
\begin{array}{l}
\textbf{ExtCallT}(\mathcal{P}, f, f', \overline{vt}) \\
\quad \textbf{assert}\ \forall vt \in \overline{vt}.vt = N \wedge \mathcal{P} = N \\
\boldsymbol{\mathcal{P}'} \longleftarrow \mathcal{P} \\
\boldsymbol{vt'} \longleftarrow \text{case } f \text{ of} \\
\quad \mathit{read\_and\_parse} \Rightarrow \mathit{vtaint} \\
\quad \_ \Rightarrow \mathit{vt}
\end{array}
$$

When two values are combined with a binary operation, the resulting value is tainted if either of them was. We define this as the *join* or *least-upper-bound* operator, $\sqcup$. We will then compare tags according to a partial order, the *no-higher-than* operator, $\sqsubseteq$. In this case, $a \sqsubseteq b$ means that a does not have higher privilege than b, and so information is allowed to flow from a to b.

$$
t_1 \sqcup t_2 \triangleq \begin{cases} \mathit{vtaint} & \text{if } t_1 = \mathit{vtaint} \\ \mathit{vtaint} & \text{if } t_2 = \mathit{vtaint} \\ N & \text{otherwise} \end{cases}
\qquad
t_1 \sqsubseteq t_2 \triangleq \begin{cases} \textbf{false} & \text{if } t_1 = \mathit{vtaint} \text{ and } t_2 = \mathit{vol} \\ \textbf{true} & \text{otherwise} \end{cases}
$$

The policy needs to failstop if a tainted value becomes visible to the outside world. That can happen when the value is passed as an argument to an external function, as we saw above, or when it is stored to volatile memory (typically representing a file or external device that might be read or might transfer.

$$
\begin{array}{l}
\textbf{BinopT}(\oplus, \mathcal{P}, vt_1, vt_2) \\
\mathcal{P}' \longleftarrow \mathcal{P} \\
vt' \longleftarrow vt_1 \sqcup vt_2
\end{array}
$$

$$
\begin{array}{l}
\textbf{StoreT}(\mathcal{P}, pt, vt_1, vt_2, \overline{lt}) \\
\quad \textbf{assert}\ \forall lt \in \overline{lt}.\mathcal{P} \sqcup pt \sqcup vt_2 \sqsubseteq lt \\
\mathcal{P}' \longleftarrow \mathcal{P} \\
vt' \longleftarrow \mathcal{P} \sqcup pt \sqcup vt_2 \\
\overline{lt}' \longleftarrow \overline{lt}
\end{array}
$$

Things become trickier when we consider that 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 tained value. At that point, any change to the machine state constitutes an information flow. This is termed an *implicit flow*.

Implicit flows become much more complex outside of expressions, when we have more complex control flow. This time the taint is carried on the PC Tag itself. When the PC Tag is tainted, all stores to memory and all updates to environments must also be tainted until all branches eventually rejoin, which might be at any point. 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 []. [TODO: this is the Denning cited in Bay and Askarov]

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. 2; `public1` must be tagged with the taint tag of `secret`, while it is safe to tag `public2` N, because that is after the join point, `J`. The same goes for fig. 3, if we are in a *termination-insensitive* setting [2]. In termination-insensitive noninterference, we allow an observer to glean information by the termination or non-termination of the program. So, it is safe to assume that the post-dominator J of the while loop is reached.

[TODO: implicit flow rules for statements]

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. 4, 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 be determined statically from a function's full control-flow graph, so we can implement it as long as we're willing to deviate from our purely syntax-based tag rules by performing a code transformation. This can be done completely automatically; for each split point in the code, the control-flow graph identifies its join point statement, and the transformation must wrap that statement in a fresh label.

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 has one—a function with multiple returns might not, in which case once the PC Tag is tainted, it must remain so until a return.

```
int f(bool secret) {
    int public1, public2;

S:  if (secret) {
b1:     public1 = 1;
    } else {
b2:     public1 = 0;
    }

J:  public2 = 42;

    return public2;
}
```

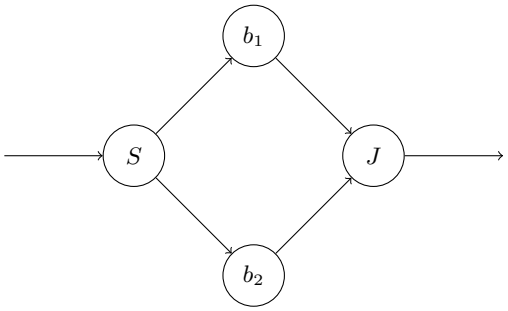


Fig. 2: Leaking via if statements

```
int f(bool secret) {
    int public1=1;
    int public2;

S:  while (secret) {
b1:     public1 = 1;
        secret = false;
    }

J:  public2 = 42;

    return public2;
}
```

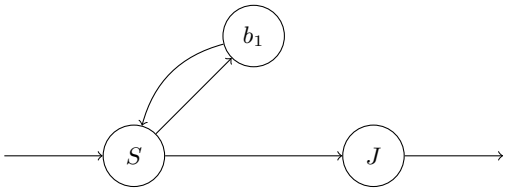


Fig. 3: Leaking via while statements

```
int f(bool secret) {
    int public1, public2;

    while (secret) {
        goto b1;
    }

b2: public1 = 1;
    goto J;

b1: public1 = 1;

J:  public2 = 42;
    return public2;
}
```

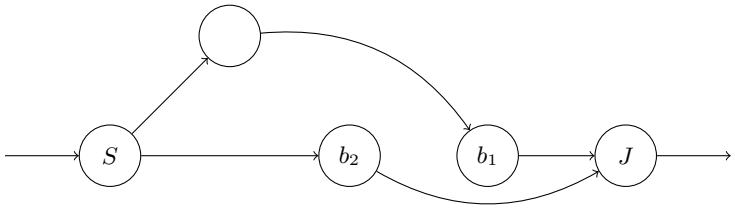
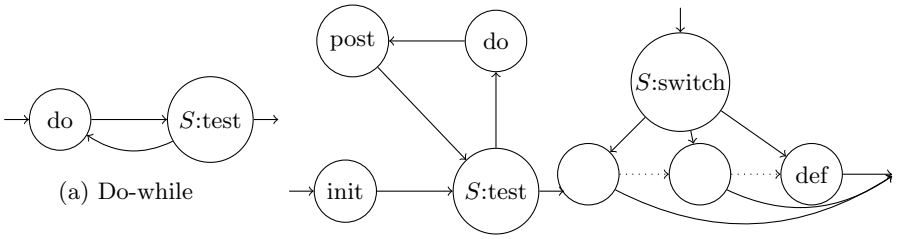


Fig. 4: Cheating with go-tos



(a) Do-while (b) For (c) Switch

Fig. 5: Remaining Branch Statements

Intransitive SIF Our second example involves information from outside of the system ending up somewhere it isn't supposed to.

```
void sanitize(buf);
char* sql_query(char* query);

void get_data() {
  char[20] name;
  char[100] query = "select address where name =";

  scanf("%19f", name);
  sanitize(name);
  strncat(query, name, strlen(name));

  sprintf(buf, sql_query(query));
  return;
}
```

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;".

In this example, we want to implement an *intransitive integrity* SIF policy: 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.

In this context, we consider the functions `scanf` and `sanitize` as sources of information, and the input to `sanitize` and `sql_query` as information "sinks."

Let Σ be the set of these three identifiers, ranged over by σ. A value may be tainted any subset of Σ, written $\mathit{vtaint}\ \overline{\sigma}$. The PC Tag tracks the current function identifier and an association list of labels and sources. Each pair (L, σ) in the association list indicates that until reaching label L, the state itself has been influenced by σ.

$$\begin{aligned}\tau ::= & \mathit{vtaint}\ \overline{id} \\ & \mathit{pc}\ f\ \mathit{ets}\overline{(L, id)} \\ & N\end{aligned}$$

We define the join operation in this new setting, as well as the *minus* operation ($t_1 - t_2$).

$$t_1 \sqcup t_2 \triangleq \begin{cases} \mathit{vtaint}\ (\overline{\sigma}_1 \cup \overline{\sigma}_2) & \text{if } t_1 = \mathit{vtaint}\ \overline{\sigma}_1 \text{ and } t_2 = \mathit{vtaint}\ \overline{\sigma}_2 \\ \mathit{vtaint}\ (\overline{\sigma}_2 \cup \{\sigma \mid (L,\sigma) \in \overline{(L,\sigma)}_1\}) & \text{if } t_1 = \mathit{pc}\ f\ \overline{(L,\sigma)}_1 \text{ and } t_2 = \mathit{vtaint}\ \overline{\sigma}_2 \\ \mathit{vtaint}\ (\overline{\sigma}_1 \cup \{\sigma \mid (L,\sigma) \in \overline{(L,\sigma)}_2\}) & \text{if } t_2 = \mathit{pc}\ f\ \overline{(L,\sigma)}_2 \text{ and } t_1 = \mathit{vtaint}\ \overline{\sigma}_1 \\ \bot & \text{otherwise} \end{cases}$$

$$t - \sigma \triangleq \begin{cases} \mathit{vtaint}\ \overline{\sigma} - \sigma & \text{if } t = \mathit{vtaint}\ \ \overline{\sigma} \\ \bot & \text{otherwise} \end{cases}$$

And once again we wish to define the "no-higher-than" relation. In this case, recall that we want to avoid the `name` argument flowing to `sql_query`. So we will define that `sql_query(query)`, as a sink, is strictly higher security than `sql_query(name)`, and every other combination is fine.

$$t_1 \sqsubseteq (t_2, t_3) \triangleq \begin{cases} \mathbf{f} & \text{if } t_1 = \mathit{vtaint}\ \overline{\sigma}, t_2 = \texttt{sql\_query}, t_3 = \texttt{query}, \text{ and } \texttt{name} \in \overline{\sigma} \\ \mathbf{t} & \text{otherwise} \end{cases}$$

Tainting and Checking Arguments and Returns A function argument or return value can be either a source or a sink. So, when they are processed by the argument and return rules, we must both check that the value being passed or returned is not tainted by a forbidden source, and then add the new source to its taint. Recall that we want the first argument to the `sanitize` function to "forget" the influence of `name`.

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

assert $\mathcal{P} \sqcup vt \sqsubseteq (f, x)$

let $vt_1 := vt - \{\texttt{santize(src)}\}$ *in*

let $vt_2 := vt_1 \sqcup \mathit{vtaint}\ \{f(x)\}$ *in*

$\boldsymbol{vt'} \longleftarrow vt_2$

$\boldsymbol{\mathcal{P}'} \longleftarrow \mathcal{P}$

$\overline{\boldsymbol{lt}} \longleftarrow [N]$

RetT$(\mathcal{P}_{CLE}, \mathcal{P}_{CLR}, vt, f)$

assert $\mathcal{P} \sqcup vt \subseteq \mathit{sink}\ (f.ret)$

let $vt_1 := vt - \{\sigma \mid \sigma / f.ret \in I\}$ *in*

let $vt_2 := vt_1 \sqcup \mathit{tainted}\ \{f.ret\}$ *in*

$\boldsymbol{vt'} \longleftarrow vt_2$

$\boldsymbol{\mathcal{P}'} \longleftarrow \mathcal{P}$

Dynamic Sinks and Globals 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. Global variables are also possible sources or sinks, so we initialize their tags to carry this information.

$$\begin{array}{l}\textbf{MallocT}(\mathcal{P}, vt)\\ \boldsymbol{pt} \longleftarrow \mathcal{P} \sqcup vtaint\ \emptyset\\ \boxed{\boldsymbol{vt}} \longleftarrow vtaint\ \emptyset\\ \boxed{\overline{\boldsymbol{lt}}} \longleftarrow [sink\ f.m]\\ \boldsymbol{\mathcal{P}'} \longleftarrow \mathcal{P}\end{array} \qquad \begin{array}{l}\textbf{GlobalT}(id, s)\\ \boldsymbol{pt} \longleftarrow vtaint\ \emptyset\\ \boldsymbol{vt} \longleftarrow vtaint\ \{id\}\\ \overline{\boldsymbol{lt}} \longleftarrow [sink\ id]\end{array}$$

PC Tag Taint It now becomes slightly more complicated to keep track of the join-point labels associated with various sources. [TODO: fix the alignment here.]

$$\begin{array}{l}\textbf{SplitT}(\mathcal{P}, vt, \boxed{L})\\ \quad let\ pc\ f\ \overline{(L,\sigma)} := \mathcal{P}\ in\\ \quad let\ vtaint\ \sigma\ :=\ vt\ in\\ \boldsymbol{\mathcal{P}'} \longleftarrow pc\ f\ (\overline{(L,\sigma)} \cup (L,\sigma))\end{array} \qquad \begin{array}{l}\textbf{LabelT}(\mathcal{P}, L)\\ let\ pc\ f\ \overline{(L,\sigma)} := \mathcal{P}\ in\\ \boldsymbol{\mathcal{P}'} \longleftarrow pc\ f\ \{(L',\sigma) \mid (L',\sigma) \in \overline{(L,\sigma)} \wedge L \neq L'\}\end{array}$$

The 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. 5, 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.

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, that the processor handles by introducing a tag corresponding to that label.

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 lower when it is reached.

5 Implementing Tagged C with PIPE

[TODO: more detailed description of Chris' work and why the optional arguments are optional]

6 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

6.1 Limitations of the Tag Mechanism

By committing to a tag-based mechanism, we do restrict the space of policies that Tagged C can enforce. In general, a reference monitor can enforce any policy that constitutes a *safety property*—any policy whose violation can be demonstrated by a single finite trace. This class includes such policies as "no integer overflow" and "pointers are always in-bounds," which depend on the values of variables. Tag-based monitors cannot enforce any policy that depends on the value of a variable rather than its tags.

7 Related Work

Reference Monitors The concept of a reference monitor was first introduced fifty years ago in [1]: 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 [7].)

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) [6] 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 [12], stack safety [11], 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.

Aspect Oriented Programming [TODO: do forward search from original AOP paper]

8 Future Work

We have presented the language and a reference interpreter, built on top of the CompCert interpreter [8], and three example policies. There are several significant next-steps.

Compilation An interpreter is all well and good, but a compiler would be preferable for many reasons. A compiled Tagged C could use the hardware acceleration of a PIPE target, and could more easily support linked libraries, including linking against code written in other languages. The ultimate goal would be a fully verified compiler, but that is a very long way off.

Language Proofs There are a couple of properties of the language semantics itself that we would like to prove. Namely (1) that its behavior (prior to adding a policy) matches that of CompCert C and (2) that the behavior of a given program is invariant under all policies up to truncation due to failstop.

Policy Correctness Proofs For each example policy discussed in this paper, we sketched a formal specification for the security property it ought to enforce. A natural continuation would be to prove the correctness of each policy against these specifications.

Policy DSL Currently, policies are written in Gallina, the language embedded in Coq. This is fine for a proof-of-concept, but not satisfactory for real use. We plan to develop a domain-specific policy language to make it easier to write Tagged C policies.

References

1. Anderson, J.P.: Computer Security Technology Planning Study. Tech. rep., U.S. Air Force Electronic Systems Division (10 1972)
2. Askarov, A., Hunt, S., Sabelfeld, A., Sands, D.: Termination-insensitive noninterference leaks more than just a bit. In: Jajodia, S., Lopez, J. (eds.) Computer Security - ESORICS 2008. pp. 333–348. Springer Berlin Heidelberg, Berlin, Heidelberg (2008)
3. Bessey, A., Block, K., Chelf, B., Chou, A., Fulton, B., Hallem, S., Henri-Gros, C., Kamsky, A., McPeak, S., Engler, D.: A few billion lines of code later: Using static analysis to find bugs in the real world. Commun. ACM **53**(2), 66–75 (feb 2010). https://doi.org/10.1145/1646353.1646374, https://doi.org/10.1145/1646353.1646374
4. Chhak, C., Tolmach, A., Anderson, S.: Towards formally verified compilation of tag-based policy enforcement. In: Proceedings of the 10th ACM SIGPLAN International Conference on Certified Programs and Proofs. p. 137–151. CPP 2021, Association for Computing Machinery, New York, NY, USA (2021). https://doi.org/10.1145/3437992.3439929, https://doi.org/10.1145/3437992.3439929
5. Denning, D.E., Denning, P.J.: Certification of programs for secure information flow. Commun. ACM **20**(7), 504–513 (jul 1977). https://doi.org/10.1145/359636.359712, https://doi.org/10.1145/359636.359712
6. Dhawan, U., Vasilakis, N., Rubin, R., Chiricescu, S., Smith, J.M., Knight Jr., T.F., Pierce, B.C., DeHon, A.: PUMP: A Programmable Unit for Metadata Processing. In: Proceedings of the Third Workshop on Hardware and Architectural Support for Security and Privacy. p. 8:1–8:8. HASP '14, ACM, New York, NY, USA (2014). https://doi.org/10.1145/2611765.2611773, http://doi.acm.org/10.1145/2611765.2611773
7. Goguen, J.A., Meseguer, J.: Security policies and security models. In: IEEE Symposium on Security and Privacy. pp. 11–20. IEEE Computer Society (1982), http://dblp.uni-trier.de/db/conf/sp/sp1982.html#GoguenM82a
8. Leroy, X.: Formal verification of a realistic compiler. Commun. ACM **52**(7), 107–115 (jul 2009). https://doi.org/10.1145/1538788.1538814, https://doi.org/10.1145/1538788.1538814
9. Munoz, D.: After all these years, the world is still powered by c programming, https://www.toptal.com/c/after-all-these-years-the-world-is-still-powered-by-c-programming
10. Overflow, S.: 2022 stack overflow annual developer survey (2022), https://survey.stackoverflow.co/2022/
11. Skorstengaard, L., Devriese, D., Birkedal, L.: StkTokens: Enforcing Well-bracketed Control Flow and Stack Encapsulation using Linear Capabilities. Proceedings of the ACM on Programming Languages **3**(POPL), 1–28 (2019)
12. Wesley Filardo, N., Gutstein, B.F., Woodruff, J., Ainsworth, S., Paul-Trifu, L., Davis, B., Xia, H., Tomasz Napierala, E., Richardson, A., Baldwin, J., Chisnall, D., Clarke, J., Gudka, K., Joannou, A., Theodore Markettos, A., Mazzinghi, A., Norton, R.M., Roe, M., Sewell, P., Son, S., Jones, T.M., Moore, S.W., Neumann, P.G., Watson, R.N.M.: Cornucopia: Temporal safety for cheri heaps. In: 2020 IEEE Symposium on Security and Privacy (SP). pp. 608–625 (2020). https://doi.org/10.1109/SP40000.2020.00098

A Syntax

$s ::=$ `Sskip`	$e ::= \mathit{Eval}\ v@vt$	Value
$\mid$ `Sdo` e	$\mid \mathit{Evar}\ x$	Variable
$\mid$ `Sseq` $s_1\ s_2$	$\mid \mathit{Efield}\ e\ id$	Field
$\mid$ `Sif`(e) `then` s_1 `else` s_2 `join` L	$\mid \mathit{EvolOf}\ e$	Load from Object
$\mid$ `Swhile`(e) `do` s `join` L	$\mid \mathit{Ederef}\ e$	Dereference Pointer
$\mid$ `Sdo` s `while` (e) `join` L	$\mid \mathit{EaddrOf}\ e$	Address of Object
$\mid$ `Sfor`$(s_1; e; s_2)$ `do` s_3 `join`	$\mid \mathit{Eunop}\ \odot\ e$	Unary Operator
$\mid$ `Sbreak`	$\mid \mathit{Ebinop}\ \oplus\ e_1\ e_2$	Binary Operator
$\mid$ `Scontinue`	$\mid \mathit{Ecast}\ e\ ty$	Cast
$\mid$ `Sreturn`	$\mid \mathit{Econd}\ e_1\ e_2\ e_3$	Conditional
$\mid$ `Sswitch` e { $\overline{(L, s)}$ } `join`	$\mid \mathit{Esize}\ ty$	Size of Type
$\mid$ `Slabel` L : s	$\mid \mathit{Ealign}\ ty$	Alignment of Type
$\mid$ `Sgoto` L	$\mid \mathit{Eassign}\ e_1\ e_2$	Assignment
	$\mid \mathit{EassignOp}\ \oplus\ e_1\ e_2$	Operator Assignment
	$\mid \mathit{EpostInc}\ \oplus\ e$	Post-Increment/Decrement
	$\mid \mathit{Ecomma}\ e_1\ e_2$	Expression Sequence
	$\mid \mathit{Ecall}\ e_f(\overline{e}_{args})$	Function Call
	$\mid \mathit{Eloc}\ l@lt$	Memory Location
	$\mid \mathit{Eparen}\ e\ ty\ t$	Parenthetical with Optional Cast

Fig. 6: Tagged C Abstract Syntax

B Continuations

$$
\begin{aligned}
k ::= & \mathit{Kemp} \\
\mid & \mathit{Kdo};\ k \\
\mid & \mathit{Kseq}\ s;\ k \\
\mid & \mathit{Kif}\ s_1\ s_2\ L;\ k \\
\mid & \mathit{KwhileTest}\ e\ s\ L;\ k \\
\mid & \mathit{KwhileLoop}\ e\ s\ L;\ k \\
\mid & \mathit{KdoWhileTest}\ e\ s\ L;\ k \\
\mid & \mathit{KdoWhileLoop}\ e\ s\ L;\ k \\
\mid & \mathit{Kfor}\ (e, s_2)\ s_3\ L;\ k \\
\mid & \mathit{KforPost}\ (e, s_2)\ s_3\ L;\ k
\end{aligned}
$$

C Initial State

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 $\mathbf{undef}@vt@\overline{lt}$ for some vt and $\overline{lt}$, 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.

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

D Step Rules

D.1 Sequencing rules

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

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

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

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

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

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

$$\frac{\mathcal{P}' \leftarrow \mathbf{LabelT}(\mathcal{P}, L)}{\mathcal{S}\,(m \mid \texttt{Slabel}\ L :\ s \gg k@\mathcal{P}) \longrightarrow \mathcal{S}\,(m \mid s \gg k@\mathcal{P}')}$$

D.2 Conditional rules

$$\frac{s = \texttt{Sif}(e)\ \texttt{then}\ s_1\ \texttt{else}\ s_2\ \texttt{join}\ L}{\mathcal{S}\,(m \mid s \gg k@\mathcal{P}) \longrightarrow \mathcal{E}\,(m \mid e \gg Kif\ s_1\ s_2\ L;\ k@\mathcal{P})}$$

$$\frac{s' = \begin{cases} s_1 & \text{if } boolof(v) = \mathbf{t} \\ s_2 & \text{if } boolof(v) = \mathbf{f} \end{cases} \qquad \mathcal{P}' \leftarrow \mathbf{SplitT}(\mathcal{P}, vt, \boxed{L})}{\mathcal{E}\,(m \mid Eval\ v@vt \gg Kif\ s_1\ s_2\ L;\ k@\mathcal{P}) \longrightarrow \mathcal{S}\,(m \mid s' \gg k@\mathcal{P}')}$$

$$\frac{}{\mathcal{S}\left(m \mid \texttt{Sswitch}\ e\ \{\ \overline{(v,s)}\ \}\ \texttt{join}\ L \gg k@\mathcal{P}\right) \longrightarrow \mathcal{E}\left(m \mid e \gg Kswitch1\ \overline{(v,s)}\ L;\ k@\mathcal{P}\right)}$$

$$\frac{select\ v\ \overline{(v,s)} = s \qquad \mathcal{P}' \leftarrow \mathbf{SplitT}(\mathcal{P}, vt, \boxed{L})}{\mathcal{E}\left(m \mid Eval\ v@vt \gg Kswitch1\ \overline{(v,s)}\ L;\ k@\mathcal{P}\right) \longrightarrow \mathcal{S}\,(m \mid s \gg Kswitch2;\ k@\mathcal{P}')}$$

$$\frac{s = \texttt{Sbreak} \vee s = \texttt{Sskip}}{\mathcal{S}\,(m \mid s \gg Kswitch2;\ k@\mathcal{P}) \longrightarrow \mathcal{S}\,(m \mid \texttt{Sskip} \gg k@\mathcal{P})}$$

$$\frac{}{\mathcal{S}\,(m \mid \texttt{Scontinue} \gg Kswitch2;\ k@\mathcal{P}) \longrightarrow \mathcal{S}\,(m \mid \texttt{Scontinue} \gg k@\mathcal{P})}$$

D.3 Loop rules

$$\frac{s = \texttt{Swhile}(e)\ \texttt{do}\ s'\ \texttt{join}\ L}{\mathcal{S}\,(m \mid s \gg k@\mathcal{P}) \longrightarrow \mathcal{E}\,(m \mid e \gg KwhileTest\ e\ s'\ L;\ k@\mathcal{P})}$$

$$\frac{\begin{array}{c} boolof(v) = \mathbf{t} \qquad k_1 = KwhileTest\ e\ s\ L;\ k \\ k_2 = KwhileLoop\ e\ s\ L;\ k \quad \mathcal{P}' \leftarrow \mathbf{SplitT}(\mathcal{P}, vt, \boxed{L}) \end{array}}{\mathcal{E}\,(m \mid Eval\ v@vt \gg k_1@\mathcal{P}) \longrightarrow \mathcal{S}\,(m \mid s \gg k_2@\mathcal{P}')}$$

$$\frac{boolof(v) = \mathbf{f}\ k = KwhileTest\ e\ s\ L;\ k'\ \mathcal{P}' \leftarrow \mathbf{SplitT}(\mathcal{P}, vt, \boxed{L})}{\mathcal{E}\,(m \mid Eval\ v@vt \gg k@\mathcal{P}) \longrightarrow \mathcal{S}\,(m \mid \texttt{Sskip} \gg k'@\mathcal{P}')}$$

$$\frac{s = \texttt{Sskip} \vee s = \texttt{Scontinue} \qquad k = KwhileLoop\ e\ s\ L;\ k'}{\mathcal{S}\,(m \mid s \gg k@\mathcal{P}) \longrightarrow \mathcal{S}\,(m \mid \texttt{Swhile}(e)\ \texttt{do}\ s\ \texttt{join}\ L \gg k'@\mathcal{P})}$$

$$\frac{k = KwhileLoop\ e\ s\ L;\ k'}{\mathcal{S}\,(m \mid \texttt{Sbreak} \gg k@\mathcal{P}) \longrightarrow \mathcal{S}\,(m \mid \texttt{Sskip} \gg k'@\mathcal{P})}$$

$$\frac{s = \texttt{Sdo}\ s'\ \texttt{while}\ (e)\ \texttt{join}\ L\ k' = KdoWhileLoop\ e\ s'\ L;\ k}{\mathcal{S}\,(m \mid s \gg k@\mathcal{P}) \longrightarrow \mathcal{S}\,(m \mid s' \gg k'@\mathcal{P})}$$

$$\frac{k_1 = KdoWhileLoop\ e\ s\ L;\ k' \qquad k_2 = KdoWhileTest\ e\ s\ L;\ k}{\mathcal{S}\,(m \mid s' = \texttt{Sskip} \vee s' = \texttt{Scontinue} \gg k_1@\mathcal{P}) \longrightarrow \mathcal{E}\,(m \mid e \gg k_2@\mathcal{P})}$$

$$\frac{boolof(v) = \mathbf{f}\ k = KdoWhileTest\ e\ s\ L;\ k'\ \mathcal{P}' \leftarrow \mathbf{SplitT}(\mathcal{P}, vt, \boxed{L})}{\mathcal{S}\,(m \mid Eval\ v@vt \gg k@\mathcal{P}) \longrightarrow \mathcal{S}\,(m \mid \texttt{Sskip} \gg k'@\mathcal{P}')}$$

$$\frac{boolof(v) = \mathbf{t}\ k = KdoWhileTest\ e\ s\ L;\ k' \qquad \mathcal{P}' \leftarrow \mathbf{SplitT}(\mathcal{P}, vt, \boxed{L})}{\mathcal{S}\,(m \mid Eval\ v@vt \gg k@\mathcal{P}) \longrightarrow \mathcal{S}\,(m \mid \texttt{Sdo}\ s\ \texttt{while}\ (e)\ \texttt{join}\ L \gg k'@\mathcal{P}')}$$

$$\frac{k = \mathit{KdoWhileLoop}\ e\ s\ L;\ k'}{\mathcal{S}\,(m \mid \texttt{Sbreak} \gg k@\mathcal{P}) \longrightarrow \mathcal{S}\,(m \mid \texttt{Sskip} \gg k'@\mathcal{P})}$$

$$\frac{s = \texttt{Sfor}(s_1; e; s_2)\ \texttt{do}\ s_3\ \texttt{join}\ L \qquad s_1 \neq \texttt{Sskip}}{\mathcal{S}\,(m \mid s \gg k@\mathcal{P}) \longrightarrow \mathcal{S}\,(m \mid s_1 \gg \mathit{Kseq}\ \texttt{Sfor}(\texttt{Sskip}; e; s_2)\ \texttt{do}\ s_3\ \texttt{join}\ L;\ k@\mathcal{P})}$$

$$\frac{s = \texttt{Sfor}(\texttt{Sskip}; e; s_2)\ \texttt{do}\ s_3\ \texttt{join}\ L}{\mathcal{S}\,(m \mid s \gg k@\mathcal{P}) \longrightarrow \mathcal{E}\,(m \mid e \gg \mathit{Kfor}\ (e, s_2)\ s_3\ L;\ k@\mathcal{P})}$$

$$\frac{\mathit{boolof}\,(v) = \mathbf{f} \qquad \mathcal{P}' \leftarrow \mathbf{SplitT}(\mathcal{P}, vt, \boxed{L})}{\mathcal{E}\,(m \mid \mathit{Eval}\ v@vt \gg \mathit{Kfor}\ (e, s_2)\ s_3\ L;\ k@\mathcal{P}) \longrightarrow \mathcal{S}\,(m \mid \texttt{Sskip} \gg k@\mathcal{P})}$$

$$\frac{k = \mathit{Kfor}\ (e, s_2)\ s_3\ L;\ k'\ \mathit{boolof}\,(v) = \mathbf{t}\ \mathcal{P}' \leftarrow \mathbf{SplitT}(\mathcal{P}, vt, \boxed{L})}{\mathcal{E}\,(m \mid \mathit{Eval}\ v@vt \gg k@\mathcal{P}) \longrightarrow \mathcal{S}\,(m \mid s_3 \gg k@\mathcal{P})}$$

$$\frac{k = \mathit{Kfor}\ (e, s_2)\ s_3\ L; \qquad s = \texttt{Sskip} \vee s = \texttt{Scontinue}}{\mathcal{S}\,(m \mid s \gg k@\mathcal{P}) \longrightarrow \mathcal{S}\,(m \mid \texttt{Sfor}(\texttt{Sskip}; e; s_2)\ \texttt{do}\ s_3\ \texttt{join}\ L \gg \mathit{KforPost}\ (e, s_2)\ s_3\ L;\ k@\mathcal{P})}$$

$$\frac{k = \mathit{Kfor}\ (e, s_1)\ s_2\ L;\ k'}{\mathcal{S}\,(m \mid \texttt{Sbreak} \gg k@\mathcal{P}) \longrightarrow \mathcal{S}\,(m \mid \texttt{Sskip} \gg k'@\mathcal{P})}$$

$$\frac{k = \mathit{KforPost}\ (e, s_2)\ s_3\ L;\ k'}{\mathcal{S}\,(m \mid \texttt{Sskip} \gg k@\mathcal{P}) \longrightarrow \mathcal{S}\,(m \mid \texttt{Sfor}(\texttt{Sskip}; e; s_2)\ \texttt{do}\ s_3\ \texttt{join}\ L \gg k@\mathcal{P})}$$

D.4 Contexts

Our expression semantics are contextual. A context *ctx* is a function from an expression to an expression and a tag. We identify a valid context using the *context* relation over a "kind" (left-hand or right-hand, LH or RH), and an expression.

$$
\begin{array}{lll}
\mathit{context}\ k\ C[e] ::= & & \\
\quad | \mathit{context}\ k\ \lambda e.e & & \\
\quad | \mathit{context}\ \textsc{lh}\ \lambda e.\mathit{Ederef}\ C[e] & & \text{where } \mathit{context}\ \textsc{rh}\ C[e] \\
\quad | \mathit{context}\ \textsc{lh}\ \lambda e.\mathit{Efield}\ C[e]\ \mathit{id} & & \text{where } \mathit{context}\ \textsc{rh}\ C[e] \\
\quad | \mathit{context}\ \textsc{rh}\ \lambda e.\mathit{EvalOf}\ C[e] & & \text{where } \mathit{context}\ \textsc{lh}\ C[e] \\
\quad | \mathit{context}\ \textsc{rh}\ \lambda e.\mathit{EaddrOf}\ C[e] & & \text{where } \mathit{context}\ \textsc{lh}\ C[e] \\
\quad | \mathit{context}\ \textsc{rh}\ \lambda e.\mathit{Eunop}\ \odot\ C[e] & & \text{where } \mathit{context}\ \textsc{rh}\ C[e] \\
\quad | \mathit{context}\ \textsc{rh}\ \lambda e.\mathit{Ebinop}\ \oplus\ C[e_1]\ e_2 & & \text{where } \mathit{context}\ \textsc{rh}\ C[e_1] \\
\quad | \mathit{context}\ \textsc{rh}\ \lambda e.\mathit{Ebinop}\ \oplus\ e_1\ C[e_2] & & \text{where } \mathit{context}\ \textsc{rh}\ C[e_2] \\
\quad | \mathit{context}\ \textsc{rh}\ \lambda e.\mathit{Ecast}\ C[e]\ \mathit{ty} & & \text{where } \mathit{context}\ \textsc{rh}\ C[e] \\
\quad | \mathit{context}\ \textsc{rh}\ \lambda e.\mathit{EseqAnd}\ C[e_1]\ e_2 & & \text{where } \mathit{context}\ \textsc{rh}\ C[e_1] \\
\quad | \mathit{context}\ \textsc{rh}\ \lambda e.\mathit{EseqOr}\ C[e_1]\ e_2 & & \text{where } \mathit{context}\ \textsc{rh}\ C[e_1] \\
\quad | \mathit{context}\ \textsc{rh}\ \lambda e.\mathit{Econd}\ C[e_1]\ e_2\ e_3 & & \text{where } \mathit{context}\ \textsc{rh}\ C[e_1] \\
\quad | \mathit{context}\ \textsc{rh}\ \lambda e.\mathit{Eassign}\ C[e_1]\ e_2 & & \text{where } \mathit{context}\ \textsc{lh}\ C[e_1] \\
\quad | \mathit{context}\ \textsc{rh}\ \lambda e.\mathit{Eassign}\ e_1\ C[e_2] & & \text{where } \mathit{context}\ \textsc{rh}\ C[e_2] \\
\quad | \mathit{context}\ \textsc{rh}\ \lambda e.\mathit{EassignOp}\ \oplus\ C[e_1]\ e_2 & & \text{where } \mathit{context}\ \textsc{lh}\ C[e_1] \\
\quad | \mathit{context}\ \textsc{rh}\ \lambda e.\mathit{EassignOp}\ \oplus\ e_1\ C[e_2] & & \text{where } \mathit{context}\ \textsc{rh}\ C[e_2] \\
\quad | \mathit{context}\ \textsc{rh}\ \lambda e.\mathit{EpostInc}\ \oplus\ C[e] & & \text{where } \mathit{context}\ \textsc{lh}\ C[e] \\
\quad | \mathit{context}\ \textsc{rh}\ \lambda e.\mathit{Ecall}\ C[e_1]\ (\overline{e_2}) & & \text{where } \mathit{context}\ \textsc{rh}\ C[e_1] \\
\quad | \mathit{context}\ \textsc{rh}\ \lambda e.\mathit{Ecall}\ e_1(C[\overline{e_2}]) & & \text{where } \mathit{context}\ \textsc{rh}\ C[e]\ \text{ for } e \in \overline{e_2} \\
\quad | \mathit{context}\ \textsc{rh}\ \lambda e.\mathit{Ecomma}\ C[e_1]\ e_2 & & \text{where } \mathit{context}\ \textsc{rh}\ C[e_1] \\
\quad | \mathit{context}\ \textsc{rh}\ \lambda e.\mathit{Eparen}\ C[e]\ \mathit{ty} & & \text{where } \mathit{context}\ \textsc{rh}\ C[e] \\
\quad | \mathit{context}\ \textsc{rh}\ \lambda e.\mathit{Eparen}\ C[e]\ \mathit{ty}\ t & & \text{where } \mathit{context}\ \textsc{rh}\ C[e]
\end{array}
$$

Next, we define a notion of expression reduction. A left-hand reduction relates an expression to an expression. A right-hand reduction relates a triple of PC Tag, memory, and expression to another such triple.

$$\frac{\mathit{context}\ \textsc{lh}\ C[e] \qquad e \Rightarrow_{\textsc{lh}} e'}{\mathcal{E}\,(m \mid C[e] \gg k@\mathcal{P}) \longrightarrow \mathcal{E}\,(m \mid C[e] \gg k@\mathcal{P})}$$

$$\frac{\mathit{context}\ \textsc{rh}\ C[e] \qquad (\mathcal{P}, m, e) \Rightarrow_{\textsc{rh}} (\mathcal{P}', m', e')}{\mathcal{E}\,(m \mid C[e] \gg k@\mathcal{P}) \longrightarrow \mathcal{E}\,(m' \mid C[e] \gg k@\mathcal{P}')}$$

D.5 Expression Rules

$$\frac{le[id] = (l, \_, pt, ty)}{\mathit{Evar}\ id \Rightarrow_{\textsc{lh}} \mathit{Eloc}\ l@pt}$$

$$\frac{le[id] = \bot \quad ge[id] = \textsc{var}(l, \_, pt, ty)}{\mathit{Evar}\ id \Rightarrow_{\textsc{lh}} \mathit{Eloc}\ l@pt}$$

$$\frac{le[id] = \bot \;\; ge[id] = \textsc{Var}(f, pt)}{Evar\ id \Rightarrow_{\textsc{Lh}} Efloc\ l@pt}$$

$$\frac{}{(\mathcal{P}, m, Ederef\ (Eval\ v@vt)) \Rightarrow_{\textsc{Rh}} (\mathcal{P}, m, Eloc\ (to\_ptr\ v)@vt)}$$

$$\frac{ty = TStruct\ id \vee ty = TUnion\ id\ offset\ id\ fld = \delta \;\; pt' \leftarrow \mathbf{FieldT}(pt, id)}{Efield\ (Eval\ p@pt : ty)\ fld) \Rightarrow_{\textsc{Lh}} Eloc\ (p + \delta)@pt'}$$

$$\frac{m[l]_{|ty|} = v@vt@\overline{lt} \qquad vt' \leftarrow \mathbf{LoadT}(\mathcal{P}, pt, vt, \overline{lt})}{(\mathcal{P}, m, EvalOf\ (Eloc\ l@pt) : ty) \Rightarrow_{\textsc{Rh}} (\mathcal{P}, m, Eval\ v@vt')}$$

$$\frac{}{(\mathcal{P}, m, EaddrOf\ (Eloc\ p@pt)) \Rightarrow_{\textsc{Rh}} (\mathcal{P}, m, Eval\ p@pt)}$$

$$\frac{\langle\odot\rangle\ v = v' \qquad vt \leftarrow \mathbf{UnopT}(\odot, \mathcal{P}, vt)}{(\mathcal{P}, m, Eunop\ \odot\ (Eval\ v@vt)) \Rightarrow_{\textsc{Rh}} (\mathcal{P}, m, Eval\ v'@vt')}$$

$$\frac{v_1\ \langle\oplus\rangle\ v_2 = v' \;\; vt' \leftarrow \mathbf{BinopT}(\oplus, \mathcal{P}, vt_1, vt_2) \quad e = Ebinop\ \oplus\ (Eval\ v_1@vt_1)\ (Eval\ v_2@vt_2)}{(\mathcal{P}, m, e) \Rightarrow_{\textsc{Rh}} (\mathcal{P}, m, Eval\ v'@vt')}$$

$$\frac{\neg isptr(ty_1)\ \neg isptr(ty_2) \qquad pt \leftarrow \mathbf{IICastT}(\mathcal{P}, vt_1)}{(\mathcal{P}, m, Ecast\ (Eval\ v@vt : ty_1)\ ty_2) \Rightarrow_{\textsc{Rh}} (\mathcal{P}, m, Eval\ v@vt' : ty_2)}$$

$$\frac{ty_1 = ptr\ ty_1' \qquad \neg isptr(ty_2) \qquad m[v]_{|ty_1'|} = \_@vt@\overline{lt} \qquad vt \leftarrow \mathbf{PICastT}(\mathcal{P}, pt, \boxed{vt, \overline{lt}})}{(\mathcal{P}, m, Ecast\ (Eval\ v@pt : ty_1)\ ty_2) \Rightarrow_{\textsc{Rh}} (\mathcal{P}, m, Eval\ v@vt' : ty_2)}$$

$$\frac{\neg isptr(ty_1) \qquad ty_2 = ptr\ ty_2' \qquad m[v]_{|ty_2'|} = \_@vt_2@\overline{lt} \qquad pt \leftarrow \mathbf{IPCastT}(\mathcal{P}, vt_1, \boxed{vt_2, \overline{lt}})}{(\mathcal{P}, m, Ecast\ (Eval\ v@vt_1 : ty_1)\ ty_2) \Rightarrow_{\textsc{Rh}} (\mathcal{P}, m, Eval\ v@pt : ty_2)}$$

$$\frac{ty_1 = ptr\ ty_1' \qquad ty_2 = ptr\ ty_2' \qquad m[v]_{|ty_1'|} = m[v]_{|ty_2'|} = \_@vt@\overline{lt} \qquad pt' \leftarrow \mathbf{PPCastT}(\mathcal{P}, pt, \boxed{vt, \overline{lt}})}{(\mathcal{P}, m, Ecast\ (Eval\ v@pt : ty_1)\ ty_2) \Rightarrow_{\textsc{Rh}} (\mathcal{P}, m, Eval\ v@pt' : ty_2)}$$

$$\frac{boolof(v) = \mathbf{t} \qquad \mathcal{P}' \leftarrow \mathbf{ExprSplitT}(\mathcal{P}, vt)}{(\mathcal{P}, m, EseqAnd\ (Eval\ v@vt)\ e) \Rightarrow_{\textsc{Rh}} (\mathcal{P}', m, Eparen\ e\ Tbool\ \mathcal{P})}$$

$$\frac{boolof(v) = \mathbf{f} \qquad \mathcal{P}' \leftarrow \mathbf{ExprSplitT}(\mathcal{P}, vt)}{(\mathcal{P}, m, EseqAnd\ (Eval\ v@vt)\ e) \Rightarrow_{\textsc{Rh}} (\mathcal{P}', m, Eparen\ (Eval\ 0@vt')\ Tbool\ \mathcal{P})}$$

$$\frac{boolof(v) = \mathbf{t} \qquad \mathcal{P}' \leftarrow \mathbf{ExprSplitT}(\mathcal{P}, vt)}{(\mathcal{P}, m, EseqOr\ (Eval\ v@vt)\ e) \Rightarrow_{\textsc{Rh}} (\mathcal{P}', m, Eparen\ (Eval\ 1@vt')\ Tbool\ \mathcal{P})}$$

$$\frac{boolof(v) = \mathbf{f} \qquad \mathcal{P}' \leftarrow \mathbf{ExprSplitT}(\mathcal{P}, vt)}{(\mathcal{P}, m, EseqOr\ (Eval\ v@vt)\ e) \Rightarrow_{\textsc{Rh}} (\mathcal{P}', m, Eparen\ e\ Tbool\ \mathcal{P})}$$

$$\frac{e' = \begin{cases} e_1 & \text{if } \mathit{boolof}(v) = \mathbf{t} \\ e_2 & \text{if } \mathit{boolof}(v) = \mathbf{f} \end{cases} \qquad \mathcal{P}' \leftarrow \mathbf{ExprSplitT}(\mathcal{P}, vt)}{(\mathcal{P}, m, \mathit{Econd}\ (\mathit{Eval}\ v@vt)\ e_1\ e_2) \Rightarrow_{\text{RH}} (\mathcal{P}', m, \mathit{Eparen}\ e'\ \ \mathcal{P}}$$

$$\frac{m[l]_{|ty|} = v_1@vt_1@\overline{lt} \qquad m' = m[l \mapsto v_2@vt'@\overline{lt}'] \qquad \mathcal{P}', vt', \overline{lt}' \leftarrow \mathbf{StoreT}(\mathcal{P}, pt, vt_1, vt_2, \overline{lt})}{(\mathcal{P}, m, \mathit{Eassign}\ (\mathit{Eloc}\ l@pt)\ (\mathit{Eval}\ v_2@vt_2)) \Rightarrow_{\text{RH}} (\mathcal{P}', m', \mathit{Eval}\ v_2@vt_2)}$$

$$\frac{m[l]_{|ty|} = v_1@vt@\overline{lt} \quad \oplus \in \{+, -, *, /, \%, <<, >>, \&, \hat{}, |\} \quad vt' \leftarrow \mathbf{LoadT}(\mathcal{P}, pt, vt, \overline{lt}) \quad e = \mathit{Eassign}\ (\mathit{Eloc}\ l@pt)\ (\mathit{Ebinop}\ \oplus\ (\mathit{Eval}\ v_1@vt')\ (\mathit{Eval}\ v_2@vt_2))}{(\mathcal{P}, m, \mathit{EassignOp}\ \oplus\ (\mathit{Eloc}\ l@pt)\ (\mathit{Eval}\ v_2@vt_2)) \Rightarrow_{\text{RH}} (\mathcal{P}, m, e)}$$

$$\frac{m[l] = v@vt@\overline{lt} \quad \oplus \in \{+, -\} \qquad vt' \leftarrow \mathbf{LoadT}(\mathcal{P}, pt, vt, \overline{lt}) \quad e = \mathit{Ecomma}\ (\mathit{Eassign}\ (\mathit{Eloc}\ l@pt)\ (\mathit{Ebinop}\ \oplus\ \mathit{Eval}\ v@vt'\ 1@def))\ (\mathit{Eval}\ v@vt')}{(\mathcal{P}, m, \mathit{EpostInc}\ \oplus\ \mathit{Eloc}\ l@pt) \Rightarrow_{\text{RH}} (\mathcal{P}, m, e)}$$

$$\frac{}{(\mathcal{P}, m, \mathit{Ecomma}\ (\mathit{Eval}\ v@vt)\ e) \Rightarrow_{\text{RH}} (\mathcal{P}, m, e)}$$

$$\frac{\mathcal{P}'', vt' \leftarrow \mathbf{ExprJoinT}(\mathcal{P}, \mathcal{P}', vt)}{(\mathcal{P}, m, \mathit{Eparen}\ e\ ty\ \mathcal{P}') \Rightarrow_{\text{RH}} (\mathcal{P}'', m, \mathit{Eval}\ v@vt')}$$

D.6 Call and Return Rules

In order to make a call, we need to reduce the function expression to an *Efloc* _@ value, an abstract location corresponding to a particular function. Then we can make the call.

$$\frac{\mathcal{P}' \leftarrow \mathbf{CallT}(\mathcal{P}, f, f')}{\mathcal{E}\ (m \mid C[\mathit{Ecall}\ \mathit{Efloc}\ f'@(\overline{v@vt})]\ ty \gg k@\mathcal{P}) \longrightarrow \mathcal{C}\ (m \mid f'(v@vt) \gg \mathit{Kcall}\ f\ C\ \mathcal{P};\ k@\mathcal{P}')}$$

When we make an internal call, we need to allocated space for locals and arguments using the helper function *frame*.

$$\mathit{frame}\ xs\ as\ m = \begin{cases} (m''[p \mapsto \mathbf{undef}@vt@\overline{lt}]_{|ty|}, \\ le'[id \mapsto (p, p + |ty|, ty, pt)]) & \text{if } xs = (id, ty) :: xs' \\ & \text{where } (m', p) \leftarrow \mathit{stack\_alloc}\ |ty|\ m, \\ & pt, vt, \overline{lt} \leftarrow \mathbf{LocalT}(\mathcal{P}, x, s), \\ & \text{and } (m'', le') = \mathit{frame}\ xs'\ as\ m' \\ (m''[p \mapsto v@vt'@\overline{lt}]_{|ty|}, \\ le'[id \mapsto (p, p + |ty|, ty, pt)]) & \text{if } as = (id, ty, v@vt) :: as' \text{ and } xs = \varepsilon \\ & \text{where } (m', p) \leftarrow \mathit{stack\_alloc}\ |ty|\ m, \\ & \mathcal{P}', pt, vt', \overline{lt} \leftarrow \mathbf{ArgT}(\mathcal{P}, vt, f, x, s), \\ & \text{and } (m'', le') = \mathit{frame}\ xs'\ as\ m' \\ (m, \lambda x.\bot) & \text{if } xs = \varepsilon \text{ and } as = \varepsilon \end{cases}$$

$$\frac{def(f) = INT(xs, as, s)\ m', le' = frame\ xs\ (zip\ as\ args)\ m\ le}{\mathcal{C}(m \mid f(args) \gg k@\mathcal{P}) \longrightarrow \mathcal{S}(m' \mid s \gg k@\mathcal{P})/le'}$$

On the other hand, when we make an external call, we step directly to a return state with some value being returned and an updated memory. [TODO: talk more about how the tag policy applies in external functions, what they can and can't do with tags.]

$$\frac{def(f) = EXT(spec)\ \mathcal{P}' \leftarrow \mathbf{ExtCallT}(\mathcal{P}, f, f', \overline{vt})\ \mathcal{P}'', m', (v@vt) = spec\ \mathcal{P}'\ args\ m}{\mathcal{C}(m \mid f(args) \gg k@\mathcal{P}) \longrightarrow \mathcal{R}(m' \mid v@vt \gg k@\mathcal{P}'')}$$

Special external functions, such as malloc, just get their own rules.

$$\frac{\mathcal{P}', pt, \boxed{vt, \overline{lt}} \leftarrow \mathbf{MallocT}(\mathcal{P}, vt) \qquad m', p \leftarrow heap\_alloc\ size\ m \qquad m'' = m'\,[p + i \mapsto (\mathbf{undef}, vt, lt)]_{size}}{\mathcal{C}(m \mid malloc((size@t)) \gg k@\mathcal{P}) \longrightarrow \mathcal{R}(m'' \mid Eval\ p@pt \gg k@\mathcal{P}')}$$

And finally, we have the return rules.

$$\frac{k = Kcall\ le'\ ctx\ \mathcal{P}_{CLR}\ k' \qquad \mathcal{P}', vt' \leftarrow \mathbf{RetT}(\mathcal{P}_{CLE}, \mathcal{P}_{CLR}, vt, f)}{\mathcal{R}(m \mid Eval\ v@vt \gg k@\mathcal{P}_{CLE}) \longrightarrow \mathcal{E}(m \mid ctx[Eval\ v@vt'] \gg k'@\mathcal{P}')/le'}$$

$$\frac{dealloc\ m\ \mathcal{P} = (\mathcal{P}', m')}{\mathcal{E}(m \mid Eval\ v@vt \gg Kreturn;\ k@\mathcal{P}) \longrightarrow \mathcal{R}(m \mid Eval\ v@vt \gg k@\mathcal{P}')}$$

$$\frac{dealloc\ m\ \mathcal{P} = (\mathcal{P}', m')}{\mathcal{S}(m \mid \texttt{Sreturn}\ \gg k@\mathcal{P}) \longrightarrow \mathcal{R}(m' \mid Eval\ \mathbf{undef}@def \gg k@\mathcal{P}')}$$

E Moved from Intro

[SNA: I'm organizing our diss tracks into paragraphs that we can cut or move as needed]

Why Dynamic? Unfortunately, it is not always possible to fully secure C code before run-time. Ideally, bugs would be quickly identified and then fixed promptly. That is not always possible for a variety of reasons: bugs may escape detection, require significant effort to diagnose, or be impractical to fix. There are many techniques for finding bugs, but there is a shared stumbling block: C is not well defined. We cannot always agree on when something is a bug in C, especially code using Undefined Behaviors (UB) [**?**]. Confusion around expected behavior is no small problem. There are 191 undefined behaviors and 52 unspecified behaviors in the C99 specification [**?**]. Sometimes these behaviors are benign and skillfully used by the developer, other times they are unintended and highly dangerous. Unfortunately the distinction between the two is easily lost. Discerning expert code review is considered best practice, although it is rarely perfectly successful [] even if an expert is available at all. Even when there is both consensus and detection of a bug[APT: ??] AN: we can find it at and we can agree its a problem that should be fixed, changing the code may not be possible because it

is in proprietary 3rd party libraries and drivers, or because regulations prohibit changes [3].

[APT: last clause is mysterious] AN: for example FDA approval used to forbid patching because you'd have to go through recertification. So healthcare wouldn't patch. SNA pointed out the coverity paper comments on this as a reason for bugs not getting fixed