A Simple Semantics and Static Analysis for Java Security

Anindya Banerjee and David A. Naumann

Stevens Institute of Technology, CS Report 2001-1

July 5, 2001

Abstract: Security in Java depends on an access control mechanism specified operationally in terms of run-time stack inspection. We give a denotational semantics in "eager" form, and show that it is equivalent to the "lazy" semantics using stack inspection. We give a static analysis of safety, *i.e.*, the absence of security errors, that is significantly simpler than previous proposals. We identify several program transformations that can be used to remove run-time checks. We give complete, detailed proofs for safety of the analysis and for the transformations, exploiting compositionality of the "eager" semantics.

This material is based upon work supported by the
National Science Foundation under Grants EIA-9806835 and INT-9813854.

A Simple Semantics and Static Analysis for Java Security

Anindya Banerjee [a,1]

[a] *Stevens Institute of Technology, Hoboken, NJ 07030 USA*

David A. Naumann [b,2]

[b] *Stevens Institute of Technology, Hoboken, NJ 07030 USA*

Abstract

Security in Java depends on an access control mechanism specified operationally in terms of run-time stack inspection. We give a denotational semantics in "eager" form, and show that it is equivalent to the "lazy" semantics using stack inspection. We give a static analysis of safety, *i.e.*, the absence of security errors, that is significantly simpler than previous proposals. We identify several program transformations that can be used to remove run-time checks. We give complete, detailed proofs for safety of the analysis and for the transformations, exploiting compositionality of the "eager" semantics.

1 Introduction

System security depends in part on protecting resources through specified access control policies. For example, a policy may allow only some users the privilege to write the password file. A typical implementation of the policy found *e.g.*, in UNIX operating systems, involves an access control list $\mathcal{A}$ which associates with each user name n their set of privileges $\mathcal{A}(n)$. When a program is running it has an associated user, normally the user who invoked the program. To write a file, a program for user n must make a system call, and that system code checks whether $\mathcal{A}(n)$ includes the privilege of writing to the

[1] Partially supported by the National Science Foundation under Grant No. EIA-9806835.

[2] Partially supported by the National Science Foundation under Grant No. INT-9813854.

file. In order for users to be able to change their passwords, the system code for this task executes in a special mode ("setuid" in UNIX); the effective user is the owner of the code (say, *root*) rather than the originator of the call (n, which can write some files but not the password file).

The Java security system is intended to offer such a mechanism in a somewhat more general form. Instead of code being owned by a user or by "the system", there can be code from a number of sources, called *principals*, which can be offered varying degrees of trust. Moreover, instead of associating a principal with a loadable executable file, principals can be associated with fragments such as class declarations. Another refinement of the Java system is that privileges must be explicitly enabled, by an operation called `doPrivileged`. The intent is that a program only enables its privileges when they are needed; this "principle of least privilege" [2] may help isolate the effect of security bugs and may facilitate static analysis. Before executing a dangerous operation, a check is made that the associated privilege has been enabled and is authorized for the current principal. This check is specified in terms of an implementation called *stack inspection*. Each stack frame is marked with the principal associated with the code for that frame, and the frame also records the privileges that have been enabled. This is used by procedure `checkPermission` which inspects the current stack.

The above description of the Java security model is an operational one. While easy to understand, it may over-constrain implementations, and it is difficult to analyze. We might question why the security model need be defined in terms of stack frames – what if we considered an implementation in which procedure calls don't always push stack? Moreover, to understand the security properties achieved and to optimize performance, we need analyses that capture the Java security model more abstractly.

Our contribution is threefold: (i) we give a denotational semantics in "eager" form, and show that it is equivalent to the "lazy" semantics using stack inspection; (ii) we give a static analysis of *safety*, *i.e.*, the absence of security errors, that is significantly simpler than previous proposals; (iii) we identify several program transformations that can be used to remove run-time checks. We give complete, detailed proofs for safety of the analysis and for the transformations, exploiting compositionality of the "eager" semantics.

Skalka and Smith [4] give an operational semantics and use it to justify a static analysis of safety specified by a type system. Their type system is complicated by the choice of using a constraint system which is basis for a type inference algorithm. We use a similar type system, but prefer to separate the specification of an analysis from algorithms to perform the analysis. We also include recursion in the language. Their semantics is easily seen to model the operational descriptions of stack inspection, but it has the usual shortcomings

of operational semantics. For example, proofs ultimately go by induction on computations; a detailed proof is not given for their safety result, presumably because it is too long to fit in a short paper. It can also be difficult to extend operational semantics to additional language features in a modular way.

Wallach, Appel and Felten [5] model the mechanism with an operational semantics that manipulates formulas in a formal logic of authentication [1]. They show that the particular logical deductions corresponding to `checkPermission` can be decided efficiently, and propose an implementation called "security passing style" in which the security state is calculated in advance. The only result proven is equivalence of the two implementations. They do not include recursion or higher order functions, and the formal semantics is not made explicit. Although the use of logic sheds some light on the security properties achieved by the mechanism, the approach requires a considerable amount of theory that is not directly germane to analyzing safety or justifying optimizations.

Security passing style seems to be a presentation of the "eager" means of evaluating security checks mentioned by Li Gong [2]. We give a simple denotational formulation of the eager semantics, using only the notions of direct interest: principals and privileges. For static analysis of safety, in the manner of Skalka and Smith, we formulate a simple syntax-directed type system and prove its soundness using the denotational semantics. We also show that the denotational semantics is equivalent to the "lazy" stack-inspection semantics, and we use the semantics to justify some program transformations that can be used to eliminate unnecessary run-time checks. The eager semantics facilitates proofs, but Java implementations use lazy semantics which appears to have better performance [2,5].

Pottier *et al.* [3] formalize the eager semantics by a translation into a lambda calculus with operations on sets. Using an operational semantics for the calculus, a proof is sketched of equivalence with stack semantics. Using a somewhat complicated general framework for typing, a static analysis is given and a safety result is sketched. The language does not include recursion.

Thanks to the simplicity of our semantics, there is no difficulty in treating language constructs such as recursion; in fact, once the meanings of types are specified, the rest of the specification (*i.e.*, meanings of expressions) follows easily. Adding state appears to be straightforward, although we follow the cited works and confine attention to applicative expressions. The simplicity of our model makes it possible to give a self-contained formal semantics and succinct but complete formal proofs. For security, one wants carefully checked proofs; the trusted computing base should be small. Simple, but adequate, formalizations are particularly crucial for the "proof carrying code" approach where proof checking is used for efficient, accurate static analysis of mobile

code at the point of deployment. The compositional nature of proofs based on denotational semantics is particularly useful in this regard.

The next section explains stack inspection informally, and it introduces our language. Section 3 gives the eager denotational semantics, Section 4 gives the static analysis, Section 5 gives example program transformations. Section 7 gives the stack semantics, and Section 8 gives examples. Section 9 concludes with a discussion.

2 Overview and language

Each declared procedure is associated with a principal n. We call n the *signer*, and write `signs` n e for a signed expression, because typically n is given by a cryptographic signature on a downloaded class file. During execution, each stack frame is labeled with the principal that signs the function, as well as the set P of privileges that have been explicitly enabled during execution of the function. For our purposes, a frame is a pair $\langle n, P\rangle$, and a nonempty stack is a list $\langle n, P\rangle :: S$ with $\langle n, P\rangle$ the top. There should be an initial stack $S_0 = \langle n_0, \varnothing\rangle :: nil$ for some designated n_0. An expression is evaluated in a stack S and with an environment h that provides values for its free variables.

Java provides operations to enable and disable a privilege, i.e., to add it to the stack frame or remove it. Normally these are used in bracketed fashion, as provided by procedure `doPrivileged` which is given a privilege p and an expression e to evaluate. It enables p, evaluates e, and then disables p. Our construct is written `dopriv` p `in` e. The effect of `dopriv` p `in` e in stack $\langle n, P\rangle :: S$ is to evaluate e in stack $\langle n, P \cup \{p\}\rangle :: S$, that is, to assert p in the current frame. (This is done regardless of whether p is authorized for n, although an equivalent effect can be obtained by asserting only authorized privileges.)

Java's `checkPermission` operation checks whether a certain privilege has been enabled and is authorized for the current principal. Checking is done by inspecting the current stack. Each dangerous code fragment should be guarded by a check for an associated privilege, so that the code cannot be executed unless the check has succeeded. This can be assured by inspection of the code, or by other forms of analysis. In our syntax, a guarded expression is written `check` p `for` e. The execution of an expression checked for privilege p is to raise a security error, which we denote by $\star$, unless the following predicate is true of p and the current stack.

$$\mathsf{chk}(p, nil) \Leftrightarrow \mathsf{false}$$
$$\mathsf{chk}(p, (\langle n, P\rangle :: S)) \Leftrightarrow p \in \mathcal{A}(n) \wedge (p \in P \vee \mathsf{chk}(p, S))$$

That is, a privilege is enabled for a particular stack, S, provided there is some frame $\langle n, P\rangle$ with $p \in P$ and p authorized for n and for all principals in frames above this one in S.

A direct implementation in these terms requires inspecting some or all of the stack frames. The implementation is "lazy" in that no checking is performed when a privilege is enabled, only when it is needed to actually perform a guarded operation. On the other hand, each check incurs a significant cost, and in secure code the checks will never fail. Static analysis can detect unnecessary checks, and justify security-preserving transformations.

A stack S determines a set $\mathsf{privs}\ S$ of enabled, authorized privileges, to wit:

$$p \in \mathsf{privs}\ S \Leftrightarrow \mathsf{chk}(p, S)$$

This gives rise to a simple form of eager semantics: instead of evaluating an expression in the context of a stack S, we use $\mathsf{privs}\ S$, along with the current principal which appears on top of S. The eager semantics is given in Section 3.

The language constructs are strict in $\star$: if a subexpression raises a security error, so does the entire expression. In Java, security errors are exceptions that can be caught. Thus it is possible for a program to determine whether a `checkPermission` operation will succeed. Rather than model the full exception mechanism, we include a construct `test` p `then` e_1 `else` e_2 which evaluates e_1 if $\mathsf{chk}(p, S)$ succeeds in the current stack S, and evaluates e_2 otherwise. Note that security error $\star$ is raised only by the `check` construct, not by `test` or `dopriv`.

In Java, the call of a procedure of a class signed by, or otherwise associated with, n, results in a new stack frame for the method, marked as owned by n. We model methods as function abstractions, but whereas Skalka and Smith use signed abstractions, we include a separate construct [3] `signs` n e. Evaluation of `signs` n e in stack S goes by evaluating e in stack $(\langle n, \varnothing\rangle :: S)$. For example, given a stack S, the evaluation of the application

$$(\texttt{fun}\ x.\ \texttt{signs}\ \mathit{user}\ \mathit{writepass}(x))\text{"myName"}$$

amounts to evaluating $\mathit{writepass}$("myName") in the stack $(\langle \mathit{user}, \varnothing\rangle :: S)$.

We separate `signs` from abstractions because it helps disentangle definitions and proofs, *e.g.*, these constructs are treated independently in our safety result.

[3] Pottier *et al.* [3] also use a separate construct for signing, but require that abstraction bodies be signed.

On the other hand, unsigned abstractions do not model the Java mechanism. In our consistency result, Theorem 7.2, we show that our semantics is equivalent to stack inspection for all *standard expressions*, *i.e.*, those in which the body of every abstraction is signed.

2.1 Syntax and typing

Given are sets Principals and Privileges, and a fixed access control list $\mathcal{A}$ that maps Principals to sets of privileges. In the grammar for data types and expressions, n ranges over Principals and p over Privileges. Application associates to the left. We include recursive definitions for expressiveness, and simple abstractions `fun` $x.\ e$ which, while expressible using `letrec`, are easier to understand in definitions and proofs. For simplicity, the only primitive type is `bool`, and the only type constructor is for functions. Products, sums, and other primitive types can be added without difficulty, as can constants besides the representative one `true`.

$$
\begin{aligned}
t ::= & \ \texttt{bool} \mid (t \to t) \\
e ::= & \ \texttt{true} \mid x \mid \texttt{if}\ e\ \texttt{then}\ e_1\ \texttt{else}\ e_2 \mid \\
& \ \texttt{fun}\ x.\ e \mid e_1\ e_2 \mid \texttt{letrec}\ f(x) = e_1\ \texttt{in}\ e_2 \mid \\
& \ \texttt{signs}\ n\ e \mid \texttt{dopriv}\ p\ \texttt{in}\ e \mid \texttt{check}\ p\ \texttt{for}\ e \mid \texttt{test}\ p\ \texttt{then}\ e_1\ \texttt{else}\ e_2
\end{aligned}
$$

A signed abstraction ${}^n\lambda x.e$ in the language of Skalka and Smith is written `fun` $x.$ `signs` $n\ e$ in ours. Surprisingly, our safety result can be proved without restriction to expressions of this form. But for the eager semantics to be equivalent to stack semantics, it is crucial that function bodies be signed so the semantics correctly tracks principals on behalf of which the body of an abstraction is evaluated.

Definition 2.1 (Standard expression)
An expression is standard if for every subexpression `fun` $x.\ e$ or `letrec` $f(x) = e$ `in` e_1 we have that e is `signs` $n\ e'$ for some n, e'.

As an example of the intended usage, we consider the problem of protecting the password file, using a privilege p for changing password and w for writing to the password file. The user is authorized to change passwords: $\mathcal{A}(user) = \{p\}$. Root is authorized to change passwords and to write the password file: $\mathcal{A}(root) = \{p, w\}$. Suppose $hwWrite$ is the operating system call which needs to be protected from direct user access. The system provides the following

code, which guards $hwWrite$ with the privilege w.

$$writepass = \texttt{fun}\ x.\ \texttt{signs}\ root\ \texttt{check}\ w\ \texttt{for}\ hwWrite(x, \text{“/etc/password”})$$
$$passwd\ \ = \texttt{fun}\ x.\ \texttt{signs}\ root\ \texttt{check}\ p\ \texttt{for dopriv}\ w\ \texttt{in}\ writepass(x)$$

Consider the following user programs.

$$bad1 = \texttt{signs}\ user\ writepass(\text{“mypass”})$$
$$bad2 = \texttt{signs}\ user\ \texttt{dopriv}\ w\ \texttt{in}\ writepass(\text{“mypass”})$$
$$use\ \ = \texttt{signs}\ user\ \texttt{dopriv}\ p\ \texttt{in}\ passwd(\text{“mypass”})$$

Here $bad1$ raises a security exception because $writepass$ checks for privilege w which is not possessed by $user$. The user can try to enable w, as in $bad2$, but because w is not authorized for $user$ the exception is still raised. By contrast, use does not raise an exception: function $passwd$ checks for privilege p which is possessed by $user$, and it enables the privilege w needed by $writepass$. Using transformations discussed in Section 5, checks that never fail can be eliminated. For example, the analysis will show that use is safe, and the transformations will reduce use to

$$\texttt{signs}\ user\ \texttt{signs}\ root\ hwWrite(\text{“mypass”}, \text{“/etc/password”})$$

Well-formed expressions are characterized by typing judgements $D \vdash e : t$ which express that e has type t where free identifiers are declared by D. A typing context D is a labeled tuple of declarations $\{x_1 : t_1, \ldots, x_k : t_k\}$. We write $D, x : t$ for the extended context $\{x_1 : t_1, \ldots, x_k : t_k, x : t\}$, and $D.x_i$ for the type of x_i. The typing rules are given in Figure 1.

3 Denotational semantics

This section gives the eager denotational semantics.

3.1 Meanings of types and type contexts

A *cpo* is a partially ordered set with least upper bounds of ascending chains; it need not have a least element. Below we define, for each type t, a cpo $[\![t]\!]$. We assume that $\bot$ and $\star$ are two values not in $\{\mathsf{true}, \mathsf{false}\}$ and not functions; this will ensure that $\{\bot, \star\} \cap [\![t]\!] = \varnothing$ for all t. We will identify $\bot$ with nontermination and $\star$ with security errors. For cpo C, define $C_{\bot\star} = C \cup \{\bot, \star\}$,

$$D \vdash \texttt{true} : \texttt{bool}$$

$$D, x : t \vdash x : t$$

$$\frac{D \vdash e : \texttt{bool} \qquad D \vdash e_1 : t \qquad D \vdash e_2 : t}{D \vdash \texttt{if}\ e\ \texttt{then}\ e_1\ \texttt{else}\ e_2 : t}$$

$$\frac{D, x : t_1 \vdash e : t_2}{D \vdash \texttt{fun}\ x.\ e : t_1 \to t_2} \qquad \frac{D \vdash e_1 : t_1 \to t_2 \qquad D \vdash e_2 : t_1}{D \vdash e_1\ e_2 : t_2}$$

$$\frac{D, f : t_1 \to t_2, x : t_1 \vdash e_1 : t_2 \qquad D, f : t_1 \to t_2 \vdash e_2 : t}{D \vdash \texttt{letrec}\ f(x) = e_1\ \texttt{in}\ e_2 : t}$$

$$\frac{D \vdash e : t}{D \vdash \texttt{signs}\ n\ e : t} \qquad \frac{D \vdash e : t}{D \vdash \texttt{dopriv}\ p\ \texttt{in}\ e : t}$$

$$\frac{D \vdash e : t}{D \vdash \texttt{check}\ p\ \texttt{for}\ e : t} \qquad \frac{D \vdash e_1 : t \qquad D \vdash e_2 : t}{D \vdash \texttt{test}\ p\ \texttt{then}\ e_1\ \texttt{else}\ e_2 : t}$$

Fig. 1. Typing rules.

ordered as the disjoint union of C with $\{\star\}$, lifted with $\bot$. That is, for any $u, v \in C_{\bot\star}$, define $u \leq v$ iff $u = \bot$, $u = v$, or u and v are in C and $u \leq v$ in C.

We define $[\![\texttt{bool}]\!] = \{\mathsf{true}, \mathsf{false}\}$, ordered by equality. We also take the powerset $\mathcal{P}(\mathsf{Privileges})$ to be a cpo ordered by equality. Define

$$[\![t_1 \to t_2]\!] = \mathcal{P}(\mathsf{Privileges}) \to [\![t_1]\!] \to [\![t_2]\!]_{\bot\star}$$

where $\to$ associates to the right and denotes continuous function space, ordered pointwise. Note that lubs are given pointwise. Also, $[\![t_1 \to t_2]\!]$ does not contain $\bot$ but it does have a least element, namely the constant function $\lambda P.\ \lambda d.\ \bot$.

Principals behave in a lexically scoped way. By contrast, privileges are dynamic and vary during execution; this is reflected in the semantics of the function type.

Let $D = \{x_1 : t_1, \ldots, x_k : t_k\}$ be a type context. Then $[\![D]\!]$ is defined to be the set $\{x_1 : [\![t_1]\!], \ldots, x_k : [\![t_k]\!]\}$ of labeled tuples of appropriate type. If h is such a record, we write $h.x_i$ for the value of field x_i. If D is the empty type context $\varnothing$, then the only element of $[\![D]\!]$ is the empty record $\{\}$. For $h \in [\![D]\!]$ and $d \in [\![t]\!]$ we write $[h \mid x \mapsto d]$ for the extended record in $[\![D, x : t]\!]$.

3.2 Meanings of expressions

An expression judgement denotes a function

$$[\![D \vdash e : t]\!] \in \mathsf{Principals} \to \mathcal{P}(\mathsf{Privileges}) \to [\![D]\!] \to [\![t]\!]_{\perp\star}$$

Given a principal n, a set $P \in \mathcal{P}(\mathsf{Privileges})$ denoting privileges required by e, and environment $h \in [\![D]\!]$, the meaning of $[\![D \vdash e : t]\!]nPh$ is either $\perp$ or $\star$ or an element of $[\![t]\!]$.

In the denotational semantics (Figure 2), we use the metalanguage construct, **let** $d = E_1$ **in** E_2, with the following semantics: if the value of E_1 is either $\perp$ or $\star$ then that is the value of the entire let expression; otherwise, its value is the value of E_2 with d bound to the value of E_1. We also write $P \sqcup_n \{p\}$ for **if** $p \in \mathcal{A}(n)$ **then** $P \cup \{p\}$ **else** P.

The semantics is standard for the most part. We will only explain the meanings of the expressions that directly concern security. In what follows, we will assume, unless otherwise stated, that expression e is signed by principal n and is computed with privilege set P and in environment h.

The meaning of `signs` n' e is the meaning of e, signed by n', computed with privilege set $P \cap \mathcal{A}(n')$, in h. To illustrate the idea, consider Li Gong's example [2, Section 3.11.2]. A game applet, *applet*, has a method that calls *FileInputStream* to open the file containing the ten current high scores. In our semantics, this scenario entails finding the meaning of `signs` *system* $FileInputStream$ by the principal *applet* under some privilege set P; and, this means we need to find the meaning of *FileInputStream* (*i.e.*, whether read privileges are enabled) under the privilege set $P \cap \mathcal{A}(system)$. Assuming *system* has all privileges, this reduces to checking if *applet* has been granted permission to read. If it has not been granted the permission, the file will not be read, even though it calls system code to do so.

The meaning of `dopriv` p `in` e is the meaning of e computed with privilege set $P \cup \{p\}$ if $p \in \mathcal{A}(n)$, and is the meaning of e computed with privilege set P if $p \notin \mathcal{A}(n)$. The meaning of `check` p `for` e is a security error if $p \notin P$; otherwise, the meaning is that of e. Finally, the meaning of `test` p `then` e_1 `else` e_2 is the meaning of e_1 or e_2 according as $p \in P$ or $p \notin P$.

We leave it to the reader to check that the semantics of each construct is a continuous function of the semantics of its constituent expressions, so the semantics of recursion is well defined.

The semantics of if-then-else is $\star$-strict in the guard but not in the branches, that being our interpretation of the metalanguage conditional.

$$
\begin{aligned}
&[\![D \vdash \texttt{true} : \texttt{bool}]\!] nPh && = \mathsf{true} \\
&[\![D, x : t \vdash x : t]\!] nPh && = h.x \\
&[\![D \vdash \texttt{if}\ e\ \texttt{then}\ e_1\ \texttt{else}\ e_2 : t]\!] nPh \\
&\quad = \mathbf{let}\ b\ =\ [\![D \vdash e : \texttt{bool}]\!] nPh\ \mathbf{in} \\
&\qquad \mathbf{if}\ b\ \mathbf{then}\ [\![D \vdash e_1 : t]\!] nPh\ \mathbf{else}\ [\![D \vdash e_2 : t]\!] nPh \\
&[\![D \vdash \texttt{fun}\ x.\ e : t_1 \to t_2]\!] nPh && = \lambda P' \in \mathcal{P}(\mathsf{Privileges}).\ \lambda d \in [\![t_1]\!]. \\
&&& \quad [\![D, x : t_1 \vdash e : t_2]\!] nP'[h \mid x \mapsto d] \\
&[\![D \vdash e_1\ e_2 : t_2]\!] nPh && = \mathbf{let}\ f\ =\ [\![D \vdash e_1 : t_1 \to t_2]\!] nPh\ \mathbf{in} \\
&&& \quad \mathbf{let}\ d = [\![D \vdash e_2 : t_1]\!] nPh\ \mathbf{in}\ fPd \\
&[\![D \vdash \texttt{letrec}\ f(x) = e_1\ \texttt{in}\ e_2 : t]\!] nPh \\
&\quad = \mathbf{let}\ G(g)\ =\ \lambda P'.\ \lambda d.\ [\![D, f : t_1 \to t_2, x : t_1 \vdash e_1 : t_2]\!] nP'[h \mid f \mapsto g, x \mapsto d]\ \mathbf{in} \\
&\qquad [\![D, f : t_1 \to t_2 \vdash e_2 : t]\!] nP[h \mid f \mapsto \mathit{fix}\, G] \\
&[\![D \vdash \texttt{signs}\ n'\ e : t]\!] nPh && = [\![D \vdash e : t]\!] n'(P \cap \mathcal{A}(n'))h \\
&[\![D \vdash \texttt{dopriv}\ p\ \texttt{in}\ e : t]\!] nPh && = [\![D \vdash e : t]\!] n(P \sqcup_n \{p\})h \\
&[\![D \vdash \texttt{check}\ p\ \texttt{for}\ e : t]\!] nPh && = \mathbf{if}\ p \in P\ \mathbf{then}\ [\![D \vdash e : t]\!] nPh\ \mathbf{else}\ \star \\
&[\![D \vdash \texttt{test}\ p\ \texttt{then}\ e_1\ \texttt{else}\ e_2 : t]\!] nPh \\
&\quad = \mathbf{if}\ p \in P\ \mathbf{then}\ [\![D \vdash e_1 : t]\!] nPh\ \mathbf{else}\ [\![D \vdash e_2 : t]\!] nPh
\end{aligned}
$$

Fig. 2. Denotational semantics

4 Static Analysis

The denotational semantics in Section 3 gives a dynamic or run-time view of safety; if a program is safe, its execution will not yield $\star$. In this section, we specify a type system that statically guarantees safety; if a program is well-typed in the system then it is safe. One may utilize the static analysis for optimizing programs *e.g.*, removing redundant checks of privileges at run-time.

The static analysis is specified by an extended form of typing judgement. The idea is to give not only the type of an expression, but a principal n and set P of privileges for which the expression is safe. An arrow type $t_1 \to t_2$ denotes functions dependent on a set of privileges, and the static analysis uses annotated types to track sets of privileges adequate for safety. We adopt a

$$\Delta;\ n \vdash \texttt{true} : \texttt{bool},\ \varnothing$$

$$\Delta, x : \theta;\ n \vdash x : \theta,\ \varnothing \qquad \frac{\Delta, x : \theta_1;\ n \vdash e : \theta_2,\ \Pi}{\Delta;\ n \vdash \texttt{fun}\ x.\ e : \theta_1 \xrightarrow{\Pi} \theta_2,\ \varnothing}$$

$$\frac{\Delta;\ n \vdash e_1 : \theta_1 \xrightarrow{\Pi} \theta_2,\ \Pi_1 \qquad \Delta;\ n \vdash e_2 : \theta_1',\ \Pi_2 \qquad \theta_1' \leq \theta_1}{\Delta;\ n \vdash e_1\ e_2 : \theta_2,\ \Pi \cup \Pi_1 \cup \Pi_2}$$

$$\frac{\Delta;\ n \vdash e : \texttt{bool},\ \Pi_1 \qquad \Delta;\ n \vdash e_1 : \theta,\ \Pi_2 \qquad \Delta;\ n \vdash e_2 : \theta,\ \Pi_3}{\Delta;\ n \vdash \texttt{if}\ e\ \texttt{then}\ e_1\ \texttt{else}\ e_2 : \theta,\ \Pi_1 \cup \Pi_2 \cup \Pi_3}$$

$$\frac{\Delta, f : \theta_1 \xrightarrow{\Pi} \theta_2, x : \theta_1;\ n \vdash e_1 : \theta_2,\ \Pi \qquad \Delta, f : \theta_1 \xrightarrow{\Pi} \theta_2;\ n \vdash e_2 : \theta,\ \Pi_1}{\Delta;\ n \vdash \texttt{letrec}\ f(x) = e_1\ \texttt{in}\ e_2 : \theta,\ \Pi \cup \Pi_1}$$

$$\frac{\Delta;\ n \vdash e : \theta,\ \Pi}{\Delta;\ n \vdash \texttt{check}\ p\ \texttt{for}\ e : \theta,\ \Pi \cup \{p\}} \qquad \frac{\Delta;\ n \vdash e : \theta,\ (\Pi \sqcup_n \{p\})}{\Delta;\ n \vdash \texttt{dopriv}\ p\ \texttt{in}\ e : \theta,\ \Pi}$$

$$\frac{\Delta;\ n' \vdash e : \theta,\ \Pi \qquad \Pi \subseteq \mathcal{A}(n')}{\Delta;\ n \vdash \texttt{signs}\ n'\ e : \theta,\ \Pi} \qquad \frac{\Delta;\ n \vdash e_1 : \theta,\ \Pi_1 \qquad \Delta;\ n \vdash e_2 : \theta,\ \Pi_2}{\Delta;\ n \vdash \texttt{test}\ p\ \texttt{then}\ e_1\ \texttt{else}\ e_2 : \theta,\ \Pi_1 \cup \Pi_2}$$

Fig. 3. Static analysis

Greek notational style for types in the static analysis. Letting Π range over sets of privileges, annotated types, θ, are defined by

$$\theta ::= \texttt{bool} \mid (\theta_1 \xrightarrow{\Pi} \theta_2)$$

For this syntax to be finitary, one could restrict Π to finite sets, but we have no need for such restriction in our proofs. An expression typed $\theta_1 \xrightarrow{\Pi} \theta_2$ signifies that its application may require at least the privileges Π for safe execution.

4.1 Type-based analysis

The analysis is specified by the typing judgement $\Delta;\ n \vdash e : \theta,\ \Pi$. In words, expression e signed by principal n and typed in context Δ, has (annotated) type θ and is safe provided at least the set Π of privileges are enabled. Figure 3 gives the specification.

Constant `true`, identifiers, and anonymous functions of the form $\texttt{fun}\ x.\ e$ are all safe: they do not require any privileges be enabled for safe execution. How-

ever, the body e in `fun` x. e, may require a set of privileges Π be enabled. This is manifest in the type $\theta_1 \xrightarrow{\Pi} \theta_2$. The latent privileges, Π, get exposed during an application, $e_1 e_2$. Say e_1 has type $\theta_1 \xrightarrow{\Pi} \theta_2$; if Π_1 may be enabled during e_1's execution, and Π_2 may be enabled during e_2's execution, then application itself may require Π be enabled; hence $\Pi \cup \Pi_1 \cup \Pi_2$ may be enabled during the execution of $e_1 e_2$. The application rule also uses subtyping, as discussed in the sequel.

The analysis for `check` p `for` e requires that in addition to privileges enabled for e, the privilege p be enabled so that the check is safe. If Π is the set of privileges that may be enabled during the execution of `dopriv` p `in` e, then p can be assumed to be enabled during the execution of e, provided $p \in \mathcal{A}(n)$.

Finally, for `signs` n' e the only privileges that should be enabled are the ones authorized for n'. Note that a signed expression can occur in a term with a different owner, so it is not the case that $\Pi \subseteq \mathcal{A}(n)$ for every derivable $\Delta; n \vdash e : \theta,\ \Pi$.

4.2 Subtyping

In contrast to the more complicated typing in Skalka and Smith, which uses a system of constraints that must be solved, [4] our analysis is syntax-directed. In some sense, our system gives minimal types and privilege assumptions. We do not formalize this notion, but informally it sheds light on the specification of the analysis. In the case of values, such as variables and abstraction, the privilege set is empty. In the case of `check` p `for` e, the rule adds the checked privilege p to the "minimal" privileges of e, and similarly for the other security constructs. In the case of conditional, a union is formed from the "minimal" privileges of the constituent expressions, and the types of the constituents are the same as the type of the conditional. By contrast, in the case of application $e_1 e_2$, the "minimal" types and privileges for e_1 and e_2 need not match exactly. So we define a relation of subtyping with the informal meaning that $\theta' \leq \theta$ provided the privileges required by θ' are contained in those required by θ. This is significant only in case e_2 has functional type, in which case the latent privileges of e_2 should be among those of e_1.

Subtyping is defined as the least relation $\leq$ with $\texttt{bool} \leq \texttt{bool}$ and, for arrow types, $\theta_1 \xrightarrow{\Pi_1} \theta_1' \leq \theta_2 \xrightarrow{\Pi_2} \theta_2'$ provided $\theta_2 \leq \theta_1$, $\theta_1' \leq \theta_2'$, and $\Pi_1 \subseteq \Pi_2$.

To relate the semantics to the static analysis, we need the ordinary type θ^* obtained by erasing annotations. This is defined by induction on θ, to wit:

[4] Pottier *et al.* [3] use unification of row variables, in a relatively complicated system.

$\texttt{bool}^* = \texttt{bool}$ and $(\theta_1 \xrightarrow{\Pi} \theta_2)^* = \theta_1^* \to \theta_2^*$. It is easy to show that if $\theta_1 \leq \theta_2$, then $\theta_1^* = \theta_2^*$.

Due to subtyping, an expression can have more than one annotated type and satisfy more than one judgement. But a derivable judgement $\Delta;\ n \vdash e : \theta,\ \Pi$ has only one derivation, which is dictated by the structure of e. Proofs in the sequel will go by "induction on e", meaning induction on the derivation of some judgement $\Delta;\ n \vdash e : \theta,\ \Pi$.

4.3 The password example

For any n, the expressions in the password example can be analyzed as follows.

$$\varnothing;\ n \vdash \mathit{writepass} : \mathit{string} \xrightarrow{\{w\}} \mathit{void},\ \varnothing$$
$$\varnothing;\ n \vdash \mathit{passwd} : \mathit{string} \xrightarrow{\{p\}} \mathit{void},\ \varnothing$$
$$\varnothing;\ n \vdash \mathit{bad}1 : \mathit{void},\ \{w\}$$
$$\varnothing;\ n \vdash \mathit{bad}2 : \mathit{void},\ \{w\}$$
$$\varnothing;\ n \vdash \mathit{use} : \mathit{void},\ \varnothing$$

4.4 Safety of the analysis

Theorem 4.1 (Safety)
Suppose $\varnothing;\ n \vdash e : \theta,\ \Pi$ is derivable. Then for all $P \in \mathcal{P}(\mathsf{Privileges})$ and $\Pi \subseteq P$, it is the case that $[\![\varnothing \vdash e : \theta^*]\!] n P\{\} \neq \star$.

Proof: Immediate consequence of Lemma 4.5 below. ■

In order to serve as an adequate induction hypothesis, the lemma strengthens the theorem by allowing judgements with non-empty contexts. But this is not enough. Values at arrow types are functions that depend on privilege sets. As induction hypothesis for the case of application we require these functions be safe with respect to the privilege set Π annotating their type.

Definition 4.2 For each annotated type θ the predicate $\mathsf{safe}\ \theta$ on $[\![\theta^*]\!]_{\perp\star}$ is defined as follows: $\mathsf{safe}\ \theta(\perp) \Leftrightarrow \mathsf{true}$ and $\mathsf{safe}\ \theta(\star) \Leftrightarrow \mathsf{false}$ for all θ. For values

other than $\bot$ and $\star$, the definition is by induction on structure of θ.

$$\begin{array}{lll} \mathsf{safe}\ \mathtt{bool}(b) & \Leftrightarrow & \mathsf{true} \\ \mathsf{safe}\ (\theta_1 \xrightarrow{\Pi} \theta_2)(f) & \Leftrightarrow & \forall P \in \mathcal{P}(\mathsf{Privileges}).\forall d \in [\![\theta_1^*]\!]. \\ & & \quad \Pi \subseteq P \wedge \mathsf{safe}\ \theta_1(d) \Rightarrow \mathsf{safe}\ \theta_2(fPd) \end{array}$$

For annotated type environment Δ, the predicate $\mathsf{safe}\ \Delta$ on $[\![\Delta^*]\!]$ is defined by $\mathsf{safe}\ \Delta(h) \Leftrightarrow \forall x \in dom(h).\mathsf{safe}(\Delta.x)(h.x)$.

Recall that $h.x \neq \bot$ and $h.x \neq \star$, because $\bot \notin [\![t]\!]$ and $\star \notin [\![t]\!]$, for all t.

Fact 4.3 $\theta \leq \theta'$ and $\mathsf{safe}\ \theta\ d$ imply $\mathsf{safe}\ \theta'\ d$.

Proof: By induction on derivation of $\theta \leq \theta'$. The result is clear for $\mathtt{bool} \leq \mathtt{bool}$. For $(\theta_1 \xrightarrow{\Pi} \theta_2) \leq (\theta_1' \xrightarrow{\Pi'} \theta_2')$, assume $\mathsf{safe}\ (\theta_1 \xrightarrow{\Pi} \theta_2)\ f$. To show $\mathsf{safe}\ (\theta_1' \xrightarrow{\Pi'} \theta_2')\ f$, consider any $P \in \mathcal{P}(\mathsf{Privileges})$, such that $\Pi' \subseteq P$, and any $d \in [\![\theta_1'^*]\!]$ with $\mathsf{safe}\ \theta_1'\ d$. From the subtyping, we know that $\Pi \subseteq \Pi'$, hence $\Pi \subseteq P$. Moreover, by induction on derivation of $\theta_1' \leq \theta_1$, we obtain $\mathsf{safe}\ \theta_1'\ d$ implies $\mathsf{safe}\ \theta_1\ d$. Hence from assumption $\mathsf{safe}\ (\theta_1 \xrightarrow{\Pi} \theta_2)\ f$, we obtain $\mathsf{safe}\ \theta_2(fPd)$ holds. Now by induction on derivation $\theta_2 \leq \theta_2'$, we obtain $\mathsf{safe}\ \theta_2'(fPd)$. ■

Lemma 4.4 The predicate safe preserves lubs. That is, for any θ, let $u : \mathbb{N} \to [\![\theta^*]\!]_{\bot\star}$ be an ascending chain. Then, $\forall i.\mathsf{safe}\ \theta\ (u_i)$ implies $\mathsf{safe}\ \theta\ (\bigsqcup_i u_i)$.

Proof: By structural induction on θ. When $\theta = \mathtt{bool}$, the assumption $\mathsf{safe}\ \theta\ (u_i)$ implies $u_i \neq \star$ for each i, so $\bigsqcup_i u_i$ is true or false or $\bot$. Thus the result holds by definition safe.
When $\theta = (\theta_1 \xrightarrow{\Pi} \theta_2)$, assume $P \in \mathcal{P}(\mathsf{Privileges})$ and $d \in [\![\theta_1^*]\!]$, such that $\Pi \subseteq P$ and $\mathsf{safe}\ \theta_1(d)$. Then, from assumption $\mathsf{safe}\ (\theta_1 \xrightarrow{\Pi} \theta_2)\ u_i$ we obtain $\mathsf{safe}\ \theta_2\ (u_iPd)$ holds for every i. Hence, by the induction hypothesis on θ_2, we get $\mathsf{safe}\ \theta_2\ (\bigsqcup_i(u_iPd))$. Because lubs are pointwise, we get $\mathsf{safe}\ \theta_2\ ((\bigsqcup_i u_i)Pd)$.
■

Lemma 4.5
Suppose $\Delta;\ n \vdash e : \theta,\ \Pi$ is derivable. Then for all $P \in \mathcal{P}(\mathsf{Privileges})$, for all $h \in [\![\Delta^*]\!]$, if $\mathsf{safe}\ \Delta(h)$ and $\Pi \subseteq P$ then $\mathsf{safe}\ \theta\ ([\![\Delta^* \vdash e : \theta^*]\!]nPh)$.

The theorem follows from the lemma because $\mathsf{safe}\ \varnothing\{\}$ and $\mathsf{safe}\ \theta([\![\varnothing \vdash e : \theta^*]\!]nP\{\})$ implies $[\![\varnothing \vdash e : \theta^*]\!]nP\{\} \neq \star$.

Another consequence of the lemma is that the language admits additional constants at all types, declared in an initial context D_0, provided the corresponding initial environment assigns a safe meaning to each identifier in D_0.

Proof: of Lemma. Go by induction on the typing derivation, $\Delta;\ n \vdash e : \theta,\ \Pi$. Throughout, we assume $P \in \mathcal{P}(\mathsf{Privileges})$ and $h \in [\![\Delta^*]\!]$ and $\mathsf{safe}\ \Delta(h)$ and $\Pi \subseteq P$, and also let $u = [\![\Delta^* \vdash e : \theta^*]\!]nPh$ for each case of e.

- Case `true`: Then, $u = \mathsf{true}$ so $\mathsf{safe}\ \mathtt{bool}(u)$ by definition safe.

- Case x: Then, $u = h.x$ and $\mathsf{safe}\ \theta(h.x)$ follows, by definition safe, from the assumption $\mathsf{safe}\ \Delta(h)$.

- Case $\mathtt{if}\ e\ \mathtt{then}\ e_1\ \mathtt{else}\ e_2$: Then $\Pi_1 \cup \Pi_2 \cup \Pi_3 \subseteq P$, and

$$u = \mathbf{if}\ b\ \mathbf{then}\ [\![\Delta^* \vdash e_1 : \theta^*]\!]nPh\ \mathbf{else}\ [\![\Delta^* \vdash e_2 : \theta^*]\!]nPh$$

  where $b = [\![\Delta^* \vdash e : \mathtt{bool}]\!]nPh$. By the induction hypothesis on the typing derivation of e, noting that $\Pi_1 \subseteq P$, we have $\mathsf{safe}\ \mathtt{bool}(b)$ and hence $b \neq \star$. If $b = \bot$ then $u = \bot$ and $\bot$ is safe. Otherwise, $b = \mathsf{true}$ or $b = \mathsf{false}$. In the former case, by the induction hypothesis on the typing derivation of e_1, noting that $\Pi_2 \subseteq P$, we have $\mathsf{safe}\ \theta(u)$. The case of $b = \mathsf{false}$ is symmetric.

- Case $\mathtt{fun}\ x.\ e$: Then $u = \lambda P'.\ \lambda d.\ [\![\Delta^*, x : \theta_1^* \vdash e : \theta_2^*]\!]nP'[h \mid x \mapsto d]$. Thus $u \neq \star$. To prove $\mathsf{safe}\ (\theta_1 \xrightarrow{\Pi} \theta_2)(u)$, consider any $P'' \in \mathcal{P}(\mathsf{Privileges})$ and any $d' \in [\![\theta_1^*]\!]$ such that $\Pi \subseteq P''$ and $\mathsf{safe}\ \theta_1(d')$, to show $\mathsf{safe}\ \theta_2(uP''d')$. By semantics, $uP''d' = [\![\Delta^*, x : \theta_1^* \vdash e : \theta_2^*]\!]nP''[h \mid x \mapsto d']$, so the induction hypothesis for e yields $\mathsf{safe}\ \theta_2(uP''d')$ provided that $\Pi \subseteq P''$ and $\mathsf{safe}\ (\Delta, x : \theta_1)[h \mid x \mapsto d']$. We have $\Pi \subseteq P''$ by assumption, and $\mathsf{safe}\ (\Delta, x : \theta_1)[h \mid x \mapsto d']$ follows from $\mathsf{safe}\ \Delta(h)$ and $\mathsf{safe}\ \theta_1(d')$.

- Case $e_1\ e_2$: Let $f = [\![\Delta^* \vdash e_1 : \theta_1^* \to \theta_2^*]\!]nPh$ and $d = [\![\Delta^* \vdash e_2 : {\theta_1'}^*]\!]nPh$, so that $u = fPd$. (Recall that $\theta_1' \leq \theta_1$ implies ${\theta_1'}^* = \theta_1^*$ so the application fPd makes sense.) From safety of h and the assumption $\Pi \cup \Pi_1 \cup \Pi_2 \subseteq P$, we get by induction on e_1 that $\mathsf{safe}\ (\theta_1 \xrightarrow{\Pi} \theta_2)(f)$, and we get $\mathsf{safe}\ \theta_1'(d)$ by induction on e_2. By $\theta_1' \leq \theta_1$ and Fact 4.3 we have $\mathsf{safe}\ \theta_1'(d) \Rightarrow \mathsf{safe}\ \theta_1(d)$. Then by definition $\mathsf{safe}\ (\theta_1 \xrightarrow{\Pi} \theta_2)(f)$ we get $\mathsf{safe}\ \theta_2(fPd)$.

- Case $\mathtt{letrec}\ f(x) = e_1\ \mathtt{in}\ e_2$: Then, $\Pi \cup \Pi_1 \subseteq P$.
  Now $u = [\![\Delta^*, f : \theta_1^* \to \theta_2^* \vdash e_2 : \theta^*]\!]nP[h \mid f \mapsto \mathit{fix}\ G]$, where
  $G(g) = \lambda P'.\ \lambda d.\ [\![\Delta^*, f : \theta_1^* \to \theta_2^*, x : \theta_1^* \vdash e_1 : \theta_2^*]\!]nP'[h \mid f \mapsto g, x \mapsto d]$. To get $\mathsf{safe}\ \theta(u)$ by induction for e_2, we need $\Pi_1 \subseteq P$ and

$$\mathsf{safe}\ (\Delta, f : \theta_1 \xrightarrow{\Pi} \theta_2)[h \mid f \mapsto \mathit{fix}\ G]$$

  The former follows from the assumption $\Pi \cup \Pi_1 \subseteq P$. The latter follows from assumption, $\mathsf{safe}\ \Delta(h)$, and $\mathsf{safe}\ (\theta_1 \xrightarrow{\Pi} \theta_2)(\mathit{fix}\ G)$. We proceed to show safety of $\mathit{fix}\ G$.

  Now $\mathit{fix}\ G = \bigsqcup_i g_i$, where $g_0 = \lambda P''.\ \lambda d \in [\![\theta_1^*]\!].\ \bot$ and $g_{i+1} = G(g_i)$. And, $\mathsf{safe}\ (\theta_1 \xrightarrow{\Pi} \theta_2)(\mathit{fix}\ G)$ is a consequence of the following claim:

$$\forall i.\ \mathsf{safe}\ (\theta_1 \xrightarrow{\Pi} \theta_2)(g_i) \tag{1}$$

Then from Lemma 4.4, we get $\mathsf{safe}\ (\theta_1 \xrightarrow{\Pi} \theta_2)(\bigsqcup_i g_i)$. It remains to show (1), for which we proceed by induction on i.
Base case: Show $\mathsf{safe}\ (\theta_1 \xrightarrow{\Pi} \theta_2)(g_0)$. Assume any $P'' \in \mathcal{P}(\mathsf{Privileges})$ and any $v \in [\![\theta_1^*]\!]$, such that $\Pi \subseteq P''$ and $\mathsf{safe}\ \theta_1(v)$. Then $g_0 P'' v = \bot \neq \star$ and $\mathsf{safe}\ \theta_2(g_0 P'' v)$ holds.
Induction step: Assume $\mathsf{safe}\ (\theta_1 \xrightarrow{\Pi} \theta_2)(g_i)$. Show $\mathsf{safe}\ (\theta_1 \xrightarrow{\Pi} \theta_2)(g_{i+1})$.
Now $g_{i+1} = G(g_i) = \lambda P'.\ \lambda d.\ [\![\Delta^*, f : \theta_1^* \to \theta_2^*, x : \theta_1^* \vdash e_1 : \theta_2^*]\!] n P[h \mid f \mapsto g_i, x \mapsto d]$. Assume any $P'' \in \mathcal{P}(\mathsf{Privileges})$ and $v \in [\![\theta_1^*]\!]$, such that $\Pi \subseteq P''$ and $\mathsf{safe}\ \theta_1(v)$. Then

$$g_{i+1} P''(v) = [\![\Delta^*, f : \theta_1^* \to \theta_2^*, x : \theta_1^* \vdash e_1 : \theta_2^*]\!] n P''[h \mid f \mapsto g_i, x \mapsto v]$$

Note that $\mathsf{safe}\ (\Delta, f : \theta_1 \xrightarrow{\Pi} \theta_2, x : \theta_1)[h \mid f \mapsto g_i, x \mapsto v]$. Therefore, by the main induction hypothesis on the typing derivation $\Delta, f : \theta_1 \xrightarrow{\Pi} \theta_2, x : \theta_1;\ n \vdash e_1 : \theta_2,\ \Pi$, since $\Pi \subseteq P$, we obtain $\mathsf{safe}\ \theta_2(g_{i+1} P'' v)$.

- Case `signs` n' e: Then $\Pi \subseteq P$ and $u = [\![\Delta^* \vdash e : \theta^*]\!] n'(P \cap \mathcal{A}(n'))h$. The induction hypothesis on the typing derivation of e can be used to obtain $\mathsf{safe}\ \theta(u)$, because $\Pi \subseteq (P \cap \mathcal{A}(n'))$ which follows from assumption $\Pi \subseteq P$ and side condition $\Pi \subseteq \mathcal{A}(n')$ on the antecedent $\Delta;\ n' \vdash e : \theta,\ \Pi$ of $\Delta;\ n \vdash \texttt{signs}\ n'\ e : \theta,\ \Pi$.

- Case `dopriv` p `in` e: Then $\Pi \subseteq P$ and $u = [\![\Delta^* \vdash e : \theta^*]\!] n(P \sqcup_n \{p\})h$. By the induction hypothesis for e, noting that $(\Pi \sqcup_n \{p\}) \subseteq (P \sqcup_n \{p\})$, we have $\mathsf{safe}\ \theta(u)$.

- Case `check` p `for` e: Then $\Pi \cup \{p\} \subseteq P$, hence $p \in P$. Now

$$u = \textbf{if}\ p \in P\ \textbf{then}\ [\![\Delta^* \vdash e : \theta^*]\!] n P h\ \textbf{else}\ \star$$

Since $p \in P$, we have, $u = [\![\Delta^* \vdash e : \theta^*]\!] n P h$ and, by the induction hypothesis on the typing derivation of e, we have $\mathsf{safe}\ \theta(u)$.

- Case `test` p `then` e_1 `else` e_2: Then $\Pi_1 \cup \Pi_2 \subseteq P$ and

$$u = \textbf{if}\ p \in P\ \textbf{then}\ [\![\Delta^* \vdash e_1 : \theta^*]\!] n P h\ \textbf{else}\ [\![\Delta^* \vdash e_2 : \theta^*]\!] n P h$$

We have two cases. Case(a): Suppose $p \in P$. Then, by induction hypothesis on typing derivation of e_1 and noting that $\Pi_1 \subseteq P$, we have $u = [\![\Delta^* \vdash e_1 : \theta^*]\!] n P h$ and $\mathsf{safe}\ \theta(u)$. Case(b), where $p \notin \mathcal{P}$, is symmetric.

■

5 Examples of program transformations

Using the eager semantics it is straightforward to justify program transformations that can be used for optimization.

First, we list a series of program transformations that move checking of privileges "outwards" from an expression.

$$\begin{array}{ll}
\texttt{if } e \texttt{ then check } p \texttt{ for } e_1 \texttt{ else check } p \texttt{ for } e_2 & = \texttt{check } p \texttt{ for if } e \texttt{ then } e_1 \texttt{ else } e_2 \\
e_1(\texttt{check } p \texttt{ for } e_2) & = \texttt{check } p \texttt{ for } e_1 e_2 \\
\texttt{test } p \texttt{ then } e_1 \texttt{ else check } p \texttt{ for } e_2 & = \texttt{check } p \texttt{ for test } p \texttt{ then } e_1 \texttt{ else } e_2 \\
\texttt{test } p' \texttt{ then check } p \texttt{ for } e_1 \texttt{ else check } p \texttt{ for } e_2 & = \texttt{check } p \texttt{ for test } p' \texttt{ then } e_1 \texttt{ else } e_2 \\
\texttt{letrec } f(x) = e_1 \texttt{ in check } p \texttt{ for } e_2 & = \texttt{check } p \texttt{ for letrec } f(x) = e_1 \texttt{ in } e_2 \\
\texttt{check } p \texttt{ for check } p \texttt{ for } e & = \texttt{check } p \texttt{ for } e \\
\texttt{signs } n \texttt{ signs } n\ e & = \texttt{signs } n\ e
\end{array}$$

These are unconditional equalities, as the reader can verify using the denotational semantics (Figure 2). Once checks have been moved outward, some can be eliminated. To eliminate a check, it must be known definitely to succeed, *e.g.*, because it has been enabled for an authorized principal. We give an example transformation of this kind in Theorem 5.4, formulated in terms of the following notions concerning expressions that do not depend on privilege p.

Definition 5.1 (p-purity) An expression e is p-pure if e has no sub-expressions of the form $\texttt{check } p \texttt{ for } e'$ or $\texttt{test } p \texttt{ then } e' \texttt{ else } e''$.

For each type t we define semantic p-purity as a predicate $\mathsf{pure}\ p\ t$ on $[\![t]\!]_{\perp\star}$, as follows: $\mathsf{pure}\ p\ t(\perp) \Leftrightarrow \mathsf{true}$ and $\mathsf{pure}\ p\ t(\star) \Leftrightarrow \mathsf{true}$ for all t. For values other than $\perp$ and $\star$, the definition is by induction on structure of t.

$$\begin{array}{lll}
\mathsf{pure}\ p\ \texttt{bool}(b) & \Leftrightarrow & \mathsf{true} \\
\mathsf{pure}\ p\ (t_1 \to t_2)(f) & \Leftrightarrow & \forall P \in \mathcal{P}(\mathsf{Privileges}).\forall d \in [\![t_1]\!]. \\
 & & \quad \mathsf{pure}\ p\ t_1(d) \Rightarrow \mathsf{pure}\ p\ t_2(fPd) \wedge fPd = f(P - \{p\})d
\end{array}$$

Finally, for environment $h \in [\![D]\!]$ we define $\mathsf{pure}\ p\ D(h)$ iff $\mathsf{pure}\ p\ t(h.x)$ for all $x : t$ in D.

Lemma 5.2 Suppose $u : \mathbb{N} \to [\![t_1 \to t_2]\!]$ is an ascending chain. Then $\forall i.\mathsf{pure}\ p\ (t_1 \to t_2)(u_i)$ implies $\mathsf{pure}\ p\ (t_1 \to t_2)(\sqcup_i u_i)$.

Proof: By definition of pure and since joins are given pointwise. ■

Lemma 5.3 If e is p-pure and typable as $D \vdash e : t$, then for all n, P, h with $\mathsf{pure}\ p\ D(h)$ we have

$$[\![D \vdash e : t]\!]nPh = [\![D \vdash e : t]\!]n(P - \{p\})h$$

and $\mathsf{pure}\ p\ t([\![D \vdash e : t]\!]nPh)$.

Proof: By induction on e. We observe for any D, n, P, h with $\mathsf{pure}\ p\ D\ (h)$

- Case `true`: The equation is direct from the semantics, which is independent of P. For p-purity of `true`, the result holds by definition of $\mathsf{pure}\ p\ \mathtt{bool}$.
- Case x: the equation is direct from the semantics which is independent of P. For p-purity of $[\![D \vdash x : t]\!]nPh$, the result holds by hypothesis on h.
- Case $\mathtt{if}\ e_1\ \mathtt{then}\ e_2\ \mathtt{else}\ e_3$: straightforward use of induction.
- Case $\mathtt{fun}\ x.\ e$: The equation holds because the semantics is independent of P. Purity holds by induction on e.
- Case $e_1 e_2$: To show the equation, we use that $[\![D \vdash e_1]\!]$ is p-pure, which holds by induction. To show purity, we again use purity of e_1 as well as purity of e_2.
- Case $\mathtt{letrec}\ f(x) = e_1\ \mathtt{in}\ e_2$: By induction on e_2, using Lemma 5.2.
- Case $\mathtt{signs}\ n'\ e$: The equation is direct from semantics, using the fact that $(P \cap \mathcal{A}(n')) - \{p\} = (P - \{p\}) \cap \mathcal{A}(n')$.
- Case $\mathtt{dopriv}\ p'\ \mathtt{in}\ e$: We first consider the case where p' is distinct from p. We have

$$\begin{aligned}
& [\![D \vdash \mathtt{dopriv}\ p'\ \mathtt{in}\ e : t]\!]nPh \\
= {} & [\![D \vdash e : t]\!]n(P \sqcup_n \{p'\})h && \text{semantics} \\
= {} & [\![D \vdash e : t]\!]n((P \sqcup_n \{p'\}) - \{p\})h && \text{induction hyp.} \\
= {} & [\![D \vdash e : t]\!]n((P - \{p\} \sqcup_n \{p'\})h && p, p' \text{distinct} \\
= {} & [\![D \vdash \mathtt{dopriv}\ p'\ \mathtt{in}\ e : t]\!]n(P - \{p\})h && \text{semantics}
\end{aligned}$$

  In case p' is p we have

$$\begin{aligned}
& [\![D \vdash \mathtt{dopriv}\ p\ \mathtt{in}\ e : t]\!]nPh \\
= {} & [\![D \vdash e : t]\!]n(P \sqcup_n \{p\})h && \text{semantics} \\
= {} & [\![D \vdash e : t]\!]n((P - \{p\}) \sqcup_n \{p\})h && \text{see below} \\
= {} & [\![D \vdash \mathtt{dopriv}\ p\ \mathtt{in}\ e : t]\!]n(P - \{p\})h && \text{semantics}
\end{aligned}$$

  The middle step is by cases on whether $p \in \mathcal{A}(n)$. If it is, the step holds by simply by definition of $\sqcup_n$. If not, the step holds by induction on e.

- Case `check` p' `for` e: Here p' is distinct from p, by p-purity. We observe

$$\begin{array}{lll}
& [\![D \vdash \texttt{check}\ p'\ \texttt{for}\ e : t]\!] n P h & \\
= & \textbf{if}\ p' \in P\ \textbf{then}\ [\![D \vdash e : t]\!] n P h\ \textbf{else}\ \star & \text{semantics} \\
= & \textbf{if}\ p' \in P - \{p\}\ \textbf{then}\ [\![D \vdash e : t]\!] n (P - \{p\}) h\ \textbf{else}\ \star & p', p \text{ distinct, ind. for } e \\
= & [\![D \vdash \texttt{check}\ p'\ \texttt{for}\ e : t]\!] n (P - \{p\}) h &
\end{array}$$

- Case `test` p' `then` e_1 `else` e_2: Again, p' is distinct from p, and the argument is similar to `check`.

■

Theorem 5.4 For all n, all $p \in \mathcal{A}(n)$, and all p-pure closed terms e

$$\texttt{signs}\ n\ \texttt{dopriv}\ p\ \texttt{in}\ \texttt{check}\ p\ \texttt{for}\ e = \texttt{signs}\ n\ e$$

Proof: Let h be the empty environment for e which is closed. We observe for any n', P:

$$\begin{array}{lll}
& [\![\texttt{signs}\ n\ \texttt{dopriv}\ p\ \texttt{in}\ \texttt{check}\ p\ \texttt{for}\ e]\!] n' P h & \\
= & [\![\texttt{dopriv}\ p\ \texttt{in}\ \texttt{check}\ p\ \texttt{for}\ e]\!] n (\mathcal{A}(n) \cap P) h & \text{by semantics} \\
= & [\![\texttt{check}\ p\ \texttt{for}\ e]\!] n ((\mathcal{A}(n) \cap P) \sqcup_n \{p\}) h & \text{semantics} \\
= & [\![\texttt{check}\ p\ \texttt{for}\ e]\!] n ((\mathcal{A}(n) \cap P) \cup \{p\}) h & p \in \mathcal{A}(n) \\
= & [\![e]\!] n ((\mathcal{A}(n) \cap P) \cup \{p\}) h & \text{semantics} \\
= & [\![e]\!] n (\mathcal{A}(n) \cap P) h & e \text{ and } h \text{ are } p\text{-pure, Lemma 5.3} \\
= & [\![\texttt{signs}\ n\ e]\!] n' P h & \text{semantics}
\end{array}$$

In the penultimate step, two uses are needed for the lemma: to remove p and, in the case that $p \in P$, to add it back. ■

Theorem 5.5 For all n, all $p \in \mathcal{A}(n)$, and all terms e

$$\texttt{signs}\ n\ \texttt{check}\ p\ \texttt{for}\ e = \texttt{check}\ p\ \texttt{for}\ \texttt{signs}\ n\ e$$

Proof: We observe for any n', P, h:

$$
\begin{array}{ll}
\quad [\![\texttt{signs}\ n\ \texttt{check}\ p\ \texttt{for}\ e]\!] n' P h & \\
= [\![\texttt{check}\ p\ \texttt{for}\ e]\!] n (P \cap \mathcal{A}(n)) h & \text{by semantics} \\
= \textbf{if}\ p \in (P \cap \mathcal{A}(n))\ \textbf{then}\ [\![e]\!] n (P \cap \mathcal{A}(n)) h\ \textbf{else}\ \star & \text{by semantics} \\
= \textbf{if}\ p \in P\ \textbf{then}\ [\![e]\!] n (P \cap \mathcal{A}(n)) h\ \textbf{else}\ \star & \text{by sets, since } p \in \mathcal{A}(n) \\
= \textbf{if}\ p \in P\ \textbf{then}\ [\![\texttt{signs}\ n\ e]\!] n' P h\ \textbf{else}\ \star & \text{by semantics} \\
= [\![\texttt{check}\ p\ \texttt{for signs}\ n\ e]\!] n' P h & \text{by semantics}
\end{array}
$$

■

The above proofs are examples of the benefit of a compositional semantics. The proofs are by direct calculation, without need for induction. For Theorem 5.4, the proof goes through for open terms as well, if the environment h is pure. One expects built-in constants to have pure and safe values.

We now work out the password example (Section 4.3) using Theorems 5.4 and 5.5. Using these theorems, we show how checks can be eliminated from the example. We abbreviate $user, root$ as u, r.

$$
\begin{array}{ll}
\quad passwd(\text{“mypass”}) & \\
= \{\text{because } passwd = (\texttt{fun}\ x.\ \texttt{signs}\ r\ \texttt{check}\ p\ \texttt{for dopriv}\ w\ \texttt{in}\ writepass(x))\} & \\
\quad \texttt{signs}\ r\ \texttt{check}\ p\ \texttt{for dopriv}\ w\ \texttt{in}\ writepass(\text{“mypass”}) & \\
= \{\text{because } writepass = (\texttt{fun}\ x.\ \texttt{signs}\ r\ \texttt{check}\ w\ \texttt{for}\ hwWrite(x, \text{“/etc/password”}))\} & \\
\quad \texttt{signs}\ r\ \texttt{check}\ p\ \texttt{for dopriv}\ w\ \texttt{in signs}\ r\ \texttt{check}\ w\ \texttt{for}\ hwWrite(\text{“mypass”}, \text{“/etc/password”}) & \\
= \{\text{by Theorem 5.5 since } \mathcal{A}(r) = \{p, w\}\} & \\
\quad \texttt{check}\ p\ \texttt{for signs}\ r\ \texttt{dopriv}\ w\ \texttt{in check}\ w\ \texttt{for signs}\ r\ hwWrite(\text{“mypass”}, \text{“/etc/password”}) & \\
= \{\text{by Theorem 5.4 since } w \in \mathcal{A}(r) \text{ and } \texttt{signs}\ r\ hwWrite(\ldots) \text{ is } p\text{-pure closed}\} & \\
\quad \texttt{check}\ p\ \texttt{for signs}\ r\ \texttt{signs}\ r\ hwWrite(\text{“mypass”}, \text{“/etc/password”}) & \\
= \{\text{because } \texttt{signs}\ n\ \texttt{signs}\ n\ e = \texttt{signs}\ n\ e\} & \\
\quad \texttt{check}\ p\ \texttt{for signs}\ r\ hwWrite(\text{“mypass”}, \text{“/etc/password”}) &
\end{array}
$$

Finally, we obtain:

$$
\begin{aligned}
& use = \texttt{signs}\ u\ \texttt{dopriv}\ p\ \texttt{in}\ passwd(\text{“mypass”}) \\
= {} & \texttt{signs}\ u\ \texttt{dopriv}\ p\ \texttt{in}\ \texttt{check}\ p\ \texttt{for}\ \texttt{signs}\ r\ hwWrite(\text{“mypass”}, \text{“/etc/password”}) \\
= {} & \{\text{by Theorem 5.4 since } p \in \mathcal{A}(u) \text{ and } \texttt{signs}\ r\ hwWrite(\ldots) \text{ is } p\text{-pure closed}\} \\
& \texttt{signs}\ u\ \texttt{signs}\ r\ hwWrite(\text{“mypass”}, \text{“/etc/password”})
\end{aligned}
$$

6 Using the Static Analysis

Section 5 gives several program transformations that can be justified by the eager denotational semantics of our language. Of what use then is the static analysis? The safety results of Section 4 show that if the static analysis derives a judgement $\Delta;\ n \vdash e : \theta, \Pi$, then executing e using a privilege set that contains at least the enabled privileges Π would not lead to a security error. We should therefore be able to drop all `dopriv`'s and `check`'s from e. If e is `test`-free, we can then show that the meaning of e is the same as its meaning with `dopriv`'s and `check`'s erased. This is formalized below.

Definition 6.1 The erasure translation $(.)^-$ is defined as follows:

$$
\begin{aligned}
& \texttt{true}^- && = \texttt{true} \\
& x^- && = x \\
& (\texttt{if}\ e_1\ \texttt{then}\ e_2\ \texttt{else}\ e_3)^- && = \texttt{if}\ e_1^-\ \texttt{then}\ e_2^-\ \texttt{else}\ e_3^- \\
& (\texttt{fun}\ x.\ e)^- && = \texttt{fun}\ x.\ e^- \\
& (\texttt{letrec}\ f(x) = e_1\ \texttt{in}\ e_2)^- && = \texttt{letrec}\ f(x) = e_1^-\ \texttt{in}\ e_2^- \\
& (\texttt{signs}\ n\ e)^- && = \texttt{signs}\ n\ e^- \\
& (\texttt{dopriv}\ p\ \texttt{in}\ e)^- && = e^- \\
& (\texttt{check}\ p\ \texttt{for}\ e)^- && = e^- \\
& (\texttt{test}\ p\ \texttt{then}\ e_1\ \texttt{else}\ e_2)^- && \text{is undefined.}
\end{aligned}
$$

Theorem 6.2 Let e be `test`-free and let $\varnothing;\ n \vdash e : \texttt{bool}, \Pi$. Then for all $P \in \mathcal{P}(\mathsf{Privileges})$, if $\Pi \subseteq P$ then $[\![\varnothing \vdash e : \texttt{bool}]\!] n P\{\} = [\![\varnothing \vdash e^- : \texttt{bool}]\!] n P\{\}$.

Proof: Immediate consequence of Lemma 6.6 and definition $\mathsf{rel}\ \texttt{bool}$ below. ■

Definition 6.3 For each annotated type θ the relation $\mathsf{rel}\ \theta$ on $[\![\theta^*]\!]_{\perp\star}$ is defined as follows: For all θ, $\mathsf{rel}\ \theta\ \perp\ \perp$ always holds and $\mathsf{rel}\ \theta\ \star\ \star$ never holds.

For values other than $\bot, \star$, the definition is by induction on structure of θ.

$$\begin{aligned}
\mathsf{rel}\ \mathtt{bool}\ b\ b' &\Leftrightarrow b = b' \\
\mathsf{rel}\ (\theta_1 \xrightarrow{\Pi} \theta_2)\ f\ f' &\Leftrightarrow \forall P \in \mathcal{P}(\mathsf{Privileges}).\forall d, d' \in [\![\theta_1^*]\!]. \\
&\qquad \Pi \subseteq P \wedge \mathsf{rel}\ \theta_1\ d\ d' \Rightarrow \mathsf{rel}\ \theta_2\ (fPd)\ (f'Pd')
\end{aligned}$$

For annotated type environment Δ, the predicate $\mathsf{rel}\ \Delta$ on $[\![\Delta^*]\!]$ is defined by $\mathsf{rel}\ \Delta\ h\ h' \Leftrightarrow dom(h) = dom(h')$ and $\forall x \in dom(h).\mathsf{rel}\ (\Delta.x)\ (h.x)\ (h'.x)$.

Fact 6.4 $\theta \leq \theta'$ and $\mathsf{rel}\ \theta\ d\ d'$ imply $\mathsf{rel}\ \theta'\ d\ d'$.

Proof: By induction on derivation of $\theta \leq \theta'$. The result is clear for $\mathtt{bool} \leq \mathtt{bool}$. For $(\theta_1 \xrightarrow{\Pi} \theta_2) \leq (\theta_1' \xrightarrow{\Pi'} \theta_2')$, assume $\mathsf{rel}\ (\theta_1 \xrightarrow{\Pi} \theta_2)\ f\ f'$. To show $\mathsf{rel}\ (\theta_1' \xrightarrow{\Pi'} \theta_2')\ f\ f'$, consider any $P \in \mathcal{P}(\mathsf{Privileges})$, such that $\Pi' \subseteq P$, and any $d, d' \in [\![\theta_1'^*]\!]$ with $\mathsf{rel}\ \theta_1'\ d\ d'$. From the subtyping, we know that $\Pi \subseteq \Pi'$, hence $\Pi \subseteq P$. Moreover, by induction on derivation of $\theta_1' \leq \theta_1$, we obtain $\mathsf{rel}\ \theta_1'\ d\ d'$ implies $\mathsf{rel}\ \theta_1\ d\ d'$. Hence from assumption $\mathsf{rel}\ (\theta_1 \xrightarrow{\Pi} \theta_2)\ f\ f'$, we obtain $\mathsf{rel}\ \theta_2(fPd)(f'Pd')$. Now by induction on derivation $\theta_2 \leq \theta_2'$, we obtain $\mathsf{rel}\ \theta_2'(fPd)(f'Pd')$. ■

Fact 6.5 The relation rel preserves lubs. That is, for any θ, let $u, u' : \mathbb{N} \to [\![\theta^*]\!]_{\bot\star}$ be ascending chains. Then, $\forall i.\mathsf{rel}\ \theta\ u_i\ u_i'$ implies $\mathsf{rel}\ \theta\ (\bigsqcup_i u_i)(\bigsqcup_i u_i')$.

Proof: By structural induction on θ. When $\theta = \mathtt{bool}$, we have $\bigsqcup_i u_i = \bigsqcup_i u_i' = \mathsf{true}$ or false or $\bot$. Thus the result holds by definition rel.
When $\theta = (\theta_1 \xrightarrow{\Pi} \theta_2)$, assume $P \in \mathcal{P}(\mathsf{Privileges})$ and $d, d' \in [\![\theta_1^*]\!]$, such that $\Pi \subseteq P$ and $\mathsf{rel}\ \theta_1 d\ d'$. Then, from assumption $\mathsf{rel}\ (\theta_1 \xrightarrow{\Pi} \theta_2)\ u_i\ u_i'$ we obtain $\mathsf{rel}\ \theta_2\ (u_iPd)(u_i'Pd')$ for every i. Hence, by the induction hypothesis on θ_2, we get $\mathsf{rel}\ \theta_2\ (\bigsqcup_i(u_iPd))(\bigsqcup_i(u_i'Pd'))$. Because lubs are pointwise, we get $\mathsf{rel}\ \theta_2\ ((\bigsqcup_i u_i)Pd)((\bigsqcup_i u_i')Pd')$. ■

Lemma 6.6 Suppose $\Delta;\ n \vdash e : \theta,\ \Pi$ is derivable and e is $\mathtt{test}$-free. Then for all $P \in \mathcal{P}(\mathsf{Privileges})$, for all $h, h^- \in [\![\Delta^*]\!]$, if $\mathsf{rel}\ \Delta\ h\ h^-$ and $\Pi \subseteq P$ then $\mathsf{rel}\ \theta\ u\ u^-$, where $u = [\![\Delta^* \vdash e : \theta^*]\!]nPh$ and $u^- = [\![\Delta^* \vdash e^- : \theta^*]\!]nPh^-$.

(Note that h^-, u^- are just suggestively named identifiers whereas e^- is the erasure of e.) The theorem follows from the lemma because $\mathsf{rel}\ \varnothing\ \{\}\ \{\}$ and by definition $\mathsf{rel}\ \mathtt{bool}$, $[\![\varnothing \vdash e : \mathtt{bool}]\!]nP\{\} = [\![\varnothing \vdash e^- : \mathtt{bool}]\!]nP\{\}$.

Proof: of Lemma. Go by induction on the typing derivation, $\Delta;\ n \vdash e : \theta,\ \Pi$. Throughout, we assume $P \in \mathcal{P}(\mathsf{Privileges})$ and $h, h^- \in [\![\Delta^*]\!]$ and $\mathsf{rel}\ \Delta\ h\ h^-$. Let $u = [\![\Delta^* \vdash e : \theta^*]\!]nPh$ and $u^- = [\![\Delta^* \vdash e^- : \theta^*]\!]nPh^-$ for each case of e.

- Case $\mathtt{true}$: Then, $u = \mathsf{true} = u^-$ and $\mathsf{rel}\ \mathtt{bool}\ u\ u^-$ by definition rel.

- Case x: Then, $u = h.x$ and $u^- = h^-.x$. And, $\mathsf{rel}\ \theta\ u\ u^-$ follows from assumption $\mathsf{rel}\ \Delta\ h\ h^-$.

- Case $\texttt{if}\ e\ \texttt{then}\ e_1\ \texttt{else}\ e_2$: Then $\Pi_1 \cup \Pi_2 \cup \Pi_3 \subseteq P$, and

$$\begin{aligned} u &= \textbf{if}\ b\ \textbf{then}\ [\![\Delta^* \vdash e_1 : \theta^*]\!] nPh\ \textbf{else}\ [\![\Delta^* \vdash e_2 : \theta^*]\!] nPh \\ u^- &= \textbf{if}\ b^-\ \textbf{then}\ [\![\Delta^* \vdash e_1^- : \theta^*]\!] nPh^-\ \textbf{else}\ [\![\Delta^* \vdash e_2^- : \theta^*]\!] nPh^- \end{aligned}$$

  where $b = [\![\Delta^* \vdash e : \texttt{bool}]\!] nPh$ and $b^- = [\![\Delta^* \vdash e^- : \texttt{bool}]\!] nPh^-$. By the induction hypothesis on the typing derivation of e, noting that $\Pi_1 \subseteq P$, we have $\mathsf{rel}\ \texttt{bool}\ b\ b^-$. If $b = \bot = b^-$ then $u = \bot = u^-$ and $\mathsf{rel}\ \theta\ \bot\ \bot$. Otherwise, $b = \mathsf{true}$ or $b = \mathsf{false}$. In the former case, by the induction hypothesis on the typing derivation of e_1, noting that $\Pi_2 \subseteq P$, we have $\mathsf{rel}\ \theta\ u\ u^-$. In the latter case, by the induction hypothesis on the typing derivation of e_2, noting that $\Pi_3 \subseteq P$, we have $\mathsf{rel}\ \theta\ u\ u^-$.

- Case $\texttt{fun}\ x.\ e$: Then

$$\begin{aligned} u &= \lambda P'.\ \lambda d.\ [\![\Delta^*, x : \theta_1^* \vdash e : \theta_2^*]\!] nP'[h \mid x \mapsto d] \\ u^- &= \lambda P'.\ \lambda d^-.\ [\![\Delta^*, x : \theta_1^* \vdash e^- : \theta_2^*]\!] nP'[h^- \mid x \mapsto d^-] \end{aligned}$$

  To prove $\mathsf{rel}\ (\theta_1 \xrightarrow{\Pi} \theta_2)\ u\ u^-$, consider any $P' \in \mathcal{P}(\mathsf{Privileges})$ and any $d, d^- \in [\![\theta_1^*]\!]$ such that $\Pi \subseteq P'$ and $\mathsf{rel}\ \theta_1\ d\ d^-$, to show $\mathsf{rel}\ \theta_2\ (uP'd')\ (u^-P'd^-)$. By semantics,

$$\begin{aligned} uP'd &= [\![\Delta^*, x : \theta_1^* \vdash e : \theta_2^*]\!] nP'[h \mid x \mapsto d] \\ u^-P'd^- &= [\![\Delta^*, x : \theta_1^* \vdash e^- : \theta_2^*]\!] nP'[h^- \mid x \mapsto d^-] \end{aligned}$$

  So the induction hypothesis for e yields $\mathsf{rel}\ \theta_2\ (uP'd)\ (u^-P'd^-)$ provided that $\Pi \subseteq P'$ and $\mathsf{rel}\ (\Delta, x : \theta_1)[h \mid x \mapsto d][h^- \mid x \mapsto d^-]$. We have $\Pi \subseteq P'$ by assumption, and $\mathsf{rel}\ (\Delta, x : \theta_1)[h \mid x \mapsto d][h^- \mid x \mapsto d^-]$ follows from $\mathsf{rel}\ \Delta\ h\ h^-$ and $\mathsf{rel}\ \theta_1\ d\ d^-$.

- Case $e_1\ e_2$: Let $f = [\![\Delta^* \vdash e_1 : (\theta_1 \xrightarrow{\Pi} \theta_2)^*]\!] nPh$ and $d = [\![\Delta^* \vdash e_2 : {\theta_1'}^*]\!] nPh$, so that $u = fPd$. Let $f^- = [\![\Delta^* \vdash e_1^- : (\theta_1 \xrightarrow{\Pi} \theta_2)^*]\!] nPh^-$ and $d^- = [\![\Delta^* \vdash e_2^- : {\theta_1'}^*]\!] nPh^-$, so that $u^- = f^-Pd^-$. (Recall that $\theta_1' \leq \theta_1$ implies ${\theta_1'}^* = \theta_1^*$ so the applications fPd and f^-Pd^- make sense.) From $\mathsf{rel}\ \Delta\ h\ h^-$ and assumption $\Pi \cup \Pi_1 \cup \Pi_2 \subseteq P$, we get by induction on e_1 that $\mathsf{rel}\ (\theta_1 \xrightarrow{\Pi} \theta_2)\ f\ f^-$, and we get $\mathsf{rel}\ \theta_1'\ d\ d^-$ by induction on e_2. By $\theta_1' \leq \theta_1$ and Fact 6.4 we have $\mathsf{rel}\ \theta_1'\ d\ d^- \Rightarrow \mathsf{rel}\ \theta_1\ d\ d^-$. Then by definition $\mathsf{rel}\ (\theta_1 \xrightarrow{\Pi} \theta_2)\ f\ f^-$, since $\Pi \subseteq P$, we get $\mathsf{rel}\ \theta_2(fPd)(f^-Pd^-)$.

- Case $\texttt{letrec}\ f(x) = e_1\ \texttt{in}\ e_2$: Then, $\Pi \cup \Pi_1 \subseteq P$.
  Now

$$u = [\![\Delta^*, f : (\theta_1 \xrightarrow{\Pi} \theta_2)* \vdash e_2 : \theta^*]\!] nP[h \mid f \mapsto \mathit{fix}\, G]$$
$$u^- = [\![\Delta^*, f : (\theta_1 \xrightarrow{\Pi} \theta_2)* \vdash e_2^- : \theta^*]\!] nP[h^- \mid f \mapsto \mathit{fix}\, G^-]$$

where

$$G(g) = \lambda P'.\ \lambda d.\ [\![\Delta^*, f : (\theta_1 \xrightarrow{\Pi} \theta_2)^*, x : \theta_1^* \vdash e_1 : \theta_2^*]\!] nP'[h \mid f \mapsto g, x \mapsto d]$$
$$G^-(g^-) = \lambda P'.\ \lambda d^-.\ [\![\Delta^*, f : (\theta_1 \xrightarrow{\Pi} \theta_2)^*, x : \theta_1^* \vdash e_1^- : \theta_2^*]\!] nP'[h^- \mid f \mapsto g^-, x \mapsto d^-]$$

To show $\mathsf{rel}\ \theta\ u\ u^-$ by induction on e_2, we need $\Pi_1 \subseteq P$ and

$$\mathsf{rel}\ (\Delta, f : \theta_1 \xrightarrow{\Pi} \theta_2)\ [h \mid f \mapsto \mathit{fix}\, G]\ [h^- \mid f \mapsto \mathit{fix}\, G^-]$$

The former follows from assumption $\Pi \cup \Pi_1 \subseteq P$. The latter follows from assumption, $\mathsf{rel}\ \Delta\ h\ h^-$, and $\mathsf{rel}\ (\theta_1 \xrightarrow{\Pi} \theta_2)(\mathit{fix}\, G)(\mathit{fix}\, G^-)$, which we now proceed to show.

Now $\mathit{fix}\, G = \bigsqcup_i g_i$, where $g_0 = \lambda P'.\ \lambda d \in [\![\theta_1^*]\!].\ \bot$ and $g_{i+1} = G(g_i)$. Also $\mathit{fix}\, G^- = \bigsqcup_i g_i^-$, where $g_0^- = \lambda P'.\ \lambda d^- \in \theta_1^*.\ \bot$ and $g_{i+1}^- = G^-(g_i^-)$. And, $\mathsf{rel}\ (\theta_1 \xrightarrow{\Pi} \theta_2)(\mathit{fix}\, G)(\mathit{fix}\, G^-)$ is a consequence of the following claim:

$$\forall i.\ \mathsf{rel}\ (\theta_1 \xrightarrow{\Pi} \theta_2)\ g_i\ g_i^- \tag{2}$$

Then from Lemma 6.5, we get $\mathsf{rel}\ (\theta_1 \xrightarrow{\Pi} \theta_2)(\bigsqcup_i g_i)(\bigsqcup_i g_i^-)$. It remains to show (2), for which we proceed by induction on i.
Base case: Show $\mathsf{rel}\ (\theta_1 \xrightarrow{\Pi} \theta_2)\ g_0\ g_0^-$. Assume any $P' \in \mathcal{P}(\mathsf{Privileges})$ and any $v, v^- \in [\![\theta_1^*]\!]$, such that $\Pi \subseteq P'$ and $\mathsf{rel}\ \theta_1\ v\ v^-$. Then $g_0 P' v = \bot = g_0^- P' v^-$ and $\mathsf{rel}\ \theta_2(g_0 P' v)(g_0^- P' v^-)$.
Induction step: Assume $\mathsf{rel}\ (\theta_1 \xrightarrow{\Pi} \theta_2)\ g_i\ g_i^-$. Show $\mathsf{rel}\ (\theta_1 \xrightarrow{\Pi} \theta_2)\ g_{i+1}\ g_{i+1}^-$. Now:

$$g_{i+1} = \lambda P'.\ \lambda d.\ [\![\Delta^*, f : (\theta_1 \xrightarrow{\Pi} \theta_2)^*, x : \theta_1^* \vdash e_1 : \theta_2^*]\!] nP[h \mid f \mapsto g_i, x \mapsto d]$$
$$g_{i+1}^- = \lambda P'.\ \lambda d^-.\ [\![\Delta^*, f : (\theta_1 \xrightarrow{\Pi} \theta_2)^*, x : \theta_1^* \vdash e_1^- : \theta_2^*]\!] nP[h^- \mid f \mapsto g_i^-, x \mapsto d^-]$$

Assume any $P' \in \mathcal{P}(\mathsf{Privileges})$ and $v, v^- \in [\![\theta_1^*]\!]$, such that $\Pi \subseteq P'$ and $\mathsf{rel}\ \theta_1\ v\ v^-$. Then

$$g_{i+1} P' v = [\![\Delta^*, f : (\theta_1 \xrightarrow{\Pi} \theta_2)^*, x : \theta_1^* \vdash e_1 : \theta_2^*]\!] nP'[h \mid f \mapsto g_i, x \mapsto v]$$
$$g_{i+1}^- P' v^- = [\![\Delta^*, f : (\theta_1 \xrightarrow{\Pi} \theta_2)^*, x : \theta_1^* \vdash e_1 : \theta_2^*]\!] nP'[h^- \mid f \mapsto g_i^-, x \mapsto v^-]$$

Note that $\mathsf{rel}\ (\Delta, f : \theta_1 \xrightarrow{\Pi} \theta_2, x : \theta_1)\ [h \mid f \mapsto g_i, x \mapsto v]\ [h^- \mid f \mapsto g_i^-, x \mapsto v^-]$. Therefore, by the main induction hypothesis on the typing derivation $\Delta, f : \theta_1 \xrightarrow{\Pi} \theta_2, x : \theta_1;\ n \vdash e_1 : \theta_2,\ \Pi$, since $\Pi \subseteq P$, we obtain $\mathsf{rel}\ \theta_2(g_{i+1} P' v)(g_{i+1}^- P' v^-)$.

- Case `signs` n' e: Then $\Pi \subseteq P$ and $u = [\![\Delta^* \vdash e : \theta^*]\!] n'(P \cap \mathcal{A}(n'))h$. The induction hypothesis on the typing derivation of e can be used to obtain

$\mathsf{rel}\ \theta\ u\ u^-$, because $\Pi \subseteq (P \cap \mathcal{A}(n'))$ which follows from assumption $\Pi \subseteq P$ and side condition $\Pi \subseteq \mathcal{A}(n')$.

- Case `dopriv` p `in` e: Then $\Pi \subseteq P$ and $u = [\![\Delta^* \vdash e : \theta^*]\!] n (P \sqcup_n \{p\}) h$. By the induction hypothesis for e, noting that $(\Pi \sqcup_n \{p\}) \subseteq (P \sqcup_n \{p\})$, we have $\mathsf{rel}\ \theta\ u\ [\![\Delta^* \vdash e^- : \theta^*]\!] n (P \sqcup_n \{p\}) h^-$. But now e^- is p-pure. So by Lemma 5.3, $[\![\Delta^* \vdash e^- : \theta^*]\!] n (P \sqcup_n \{p\}) h^- = [\![\Delta^* \vdash e^- : \theta^*]\!] n P h^-$. But $u^- = [\![\Delta^* \vdash e^- : \theta^*]\!] n P h^-$. Hence $\mathsf{rel}\ \theta\ u\ u^-$.

- Case `check` p `for` e: Then $\Pi \cup \{p\} \subseteq P$, hence $p \in P$. Now

$$u = \mathbf{if}\ p \in P\ \mathbf{then}\ [\![\Delta^* \vdash e : \theta^*]\!] n P h\ \mathbf{else}\ \star$$

  Since $p \in P$, we have, $u = [\![\Delta^* \vdash e : \theta^*]\!] n P h$ and, by the induction hypothesis on the typing derivation of e, we have $\mathsf{rel}\ \theta\ u\ [\![\Delta^* \vdash e^- : \theta^*]\!] n P h^-$. Hence $\mathsf{rel}\ \theta\ u\ u^-$.

■

7 Stack Semantics

This section gives a formal semantics using stack inspection, and shows that for standard expressions it coincides with the eager semantics. The connection is much more direct than that of Wallach, Appel and Felten, so a complete detailed proof is not very lengthy.

Because the operations on the stack are in fact stack-like, it is straightforward to give a denotational style semantics parameterized on the stack. We define $\mathsf{Stacks} = \mathsf{nonempty\ list\ of}(\mathsf{Principals} \times \mathcal{P}(\mathsf{Privileges}))$, taken as a cpo ordered by equality. The top is the head of the list, and we write infix :: for cons, so $\langle n, P\rangle :: S$ is the stack with $\langle n, P\rangle$ on top of S, as in Section 2. We also use the predicate chk defined there, and recall the definition $p \in \mathsf{privs}\ S \Leftrightarrow \mathsf{chk}(p, S)$.

Fact 7.1 For all S and all n we have $\mathsf{privs}(S) \cap \mathcal{A}(n) = \mathsf{privs}(\langle n, \varnothing\rangle :: S)$.

Proof: The sets are equal because for any p

$$\begin{array}{lll}
p \in \mathsf{privs}(\langle n, \varnothing\rangle :: S) & \Leftrightarrow\ \mathsf{chk}(p, (\langle n, \varnothing\rangle :: S)) & \text{by def } \mathsf{privs} \\
& \Leftrightarrow\ p \in \mathcal{A}(n) \wedge \mathsf{chk}(p, S) & \text{by def } \mathsf{chk} \text{ and } p \notin \varnothing \\
& \Leftrightarrow\ p \in \mathcal{A}(n) \wedge p \in \mathsf{privs}(S) & \text{by def } \mathsf{privs}
\end{array}$$

■

$$
\begin{array}{lll}
(\!|D \vdash \texttt{true} : \texttt{bool}|\!)Sh & = \mathsf{true} \\
(\!|D \vdash x : t|\!)Sh & = h.x \\
(\!|D \vdash \texttt{if}\ e\ \texttt{then}\ e_1\ \texttt{else}\ e_2 : t|\!)Sh & = \textbf{let}\ b\ =\ (\!|D \vdash e : \texttt{bool}|\!)Sh\ \textbf{in} \\
 & \quad \textbf{if}\ b\ \textbf{then}\ (\!|D \vdash e_1 : t|\!)Sh\ \textbf{else}\ (\!|D \vdash e_2 : t|\!)Sh \\
(\!|D \vdash \texttt{fun}\ x.\ e : t_1 \to t_2|\!)Sh & = \lambda S' \in \mathsf{Stacks}.\ \lambda d \in (\!|t_1|\!).\ \\
 & \quad (\!|D, x : t_1 \vdash e : t_2|\!)S'[h \mid x \mapsto d] \\
(\!|D \vdash e_1\ e_2 : t_2|\!)Sh & = \textbf{let}\ f\ =\ (\!|D \vdash e_1 : t_1 \to t_2|\!)Sh\ \textbf{in} \\
 & \quad \textbf{let}\ d = (\!|D \vdash e_2 : t_1|\!)Sh\ \textbf{in}\ fSd \\
(\!|D \vdash \texttt{letrec}\ f(x) = e_1\ \texttt{in}\ e_2 : t|\!)Sh & \\
\quad = \textbf{let}\ G(g)\ =\ \lambda S'.\ \lambda d.\ (\!|D, f : t_1 \to t_2, x : t_1 \vdash e_1 : t_2|\!)S[h \mid f \mapsto g, x \mapsto d]\ \textbf{in} & \\
\quad\ (\!|D, f : t_1 \to t_2 \vdash e_2 : t|\!)S[h \mid f \mapsto \mathit{fix}\, G] & \\
(\!|D \vdash \texttt{signs}\ n'\ e : t|\!)Sh & = (\!|D \vdash e : t|\!)(\langle n', \varnothing\rangle :: S)h \\
(\!|D \vdash \texttt{dopriv}\ p\ \texttt{in}\ e : t|\!)(\langle n, P\rangle :: S)h & = (\!|D \vdash e : t|\!)(\langle n, P \cup \{p\}\rangle :: S)h \\
(\!|D \vdash \texttt{check}\ p\ \texttt{for}\ e : t|\!)Sh & = \textbf{if}\ \mathsf{chk}(p, S)\ \textbf{then}\ (\!|D \vdash e : t|\!)Sh\ \textbf{else}\ \star \\
(\!|D \vdash \texttt{test}\ p\ \texttt{then}\ e_1\ \texttt{else}\ e_2 : t|\!)Sh & = \textbf{if}\ \mathsf{chk}(p, S)\ \textbf{then}\ (\!|D \vdash e_1 : t|\!)Sh\ \textbf{else}\ (\!|D \vdash e_2 : t|\!)Sh
\end{array}
$$

Fig. 4. Stack semantics

The stack semantics of an expression is a function

$$(\!|D \vdash e : t|\!) \in \mathsf{Stacks} \to (\!|D|\!) \to (\!|t|\!)_{\perp\star}$$

Just as in the eager semantics, we need to account for dynamic binding of privileges by interpreting arrow types using an extra parameter. The stack semantics of types is as follows.

$$
\begin{array}{ll}
(\!|\texttt{bool}|\!) & = \{\mathsf{true}, \mathsf{false}\} \\
(\!|t_1 \to t_2|\!) & = \mathsf{Stacks} \to (\!|t_1|\!) \to (\!|t_2|\!)_{\perp\star}
\end{array}
$$

The semantics of expressions is in Figure 4.

We can now relate the denotational semantics of Figure 2 to the stack semantics of Figure 4.

Theorem 7.2 (Consistency)

For any standard expression e and stack $(\langle n, P'\rangle :: S)$, we have

$$[\![\varnothing \vdash e : \texttt{bool}]\!] n P \{\} \;=\; (\!|\varnothing \vdash e : \texttt{bool}|\!)(\langle n, P'\rangle :: S)\{\}$$

where $P = \mathsf{privs}(\langle n, P'\rangle :: S)$.

Proof: Immediate consequence of Lemma 7.5 and definition sim bool below. ■

As in the proof of safety, we need to generalize the result to allow nonempty contexts. We also consider expressions of arrow type, for which a logical relation is needed.

Definition 7.3 Define data-type indexed family $\mathsf{sim}\ t \subseteq [\![t]\!]_{\perp\star} \times (\!|t|\!)_{\perp\star}$ as follows.

$$\begin{aligned}
\mathsf{sim}\ t\ \perp\ \perp &\Leftrightarrow \mathsf{true}\\
\mathsf{sim}\ t\ \star\ \star &\Leftrightarrow \mathsf{true}\\
\mathsf{sim}\ \texttt{bool}\ b\ b' &\Leftrightarrow b = b'\\
\mathsf{sim}\ (t_1 \to t_2)\ f\ f' &\Leftrightarrow \forall S \in \mathsf{Stacks}.\forall d \in [\![t_1]\!].\forall d' \in (\!|t_1|\!).\\
&\qquad \mathsf{sim}\ t_1\ d\ d' \Rightarrow \mathsf{sim}\ t_2\ (f\ (\mathsf{privs}\ S)\ d)\ (f'\ S\ d')
\end{aligned}$$

An environment $h \in [\![D]\!]$ simulates an environment $h' \in (\!|D|\!)$, written $\mathsf{sim}\ D\ h\ h'$, provided $\mathsf{sim}\ (D.x)\ (h.x)\ (h'.x)$ for all $x \in dom(h)$.

Lemma 7.4 The relation sim preserves lubs. That is, for any t, if $u : \mathbb{N} \to [\![t]\!]$ and $u' : \mathbb{N} \to (\!|t|\!)$ are ascending chains and $\forall i.\mathsf{sim}\ t\ u_i\ u'_i$ then $\mathsf{sim}\ t\ (\bigsqcup_i u_i)\ (\bigsqcup_i u'_i)$.

Proof: Go by structural induction on t. Assume that $\mathsf{sim}\ t\ u_i\ u'_i$. When $t = \texttt{bool}$, by definition sim we obtain, for each i, $u_i = u'_i$. Thus $\mathsf{sim}\ t\ (\bigsqcup_i u_i)\ (\bigsqcup_i u'_i)$.

When $t = t_1 \to t_2$, consider any P, S, d, d' with $P = \mathsf{privs}(S)$ and $\mathsf{sim}\ t_1\ d\ d'$. We must show $\mathsf{sim}\ t_2\ ((\bigsqcup_i u_i)Pd)\ ((\bigsqcup_i u'_i)Sd')$, *i.e.*, by definition of lubs we must show, $\mathsf{sim}\ t_2\ \bigsqcup_i(u_iPd)\ \bigsqcup_i(u'_iSd')$. By assumption, for every i, $\mathsf{sim}\ (t_1 \to t_2)\ u_i\ u'_i$, hence, $\mathsf{sim}\ t_2\ (u_iPd)\ (u'_iSd')$ holds for each i. Therefore, by induction for t_2, we obtain $\mathsf{sim}\ t_2\ \bigsqcup_i(u_iPd)\ \bigsqcup_i(u'_iSd')$. ■

Lemma 7.5 For any stack $(\langle n, P'\rangle :: S)$, for any standard expression e, and any D, t, h, h', let $u = [\![D \vdash e : t]\!] n P h$ where $P = \mathsf{privs}(\langle n, P'\rangle :: S)$, and let

$$u' = (\!|D \vdash e : t|\!)(\langle n, P'\rangle :: S)h'$$

Then $\mathsf{sim}\ D\ h\ h' \Rightarrow \mathsf{sim}\ t\ u\ u'$.

The Consistency Theorem follows from the lemma because $\mathsf{sim}\ \varnothing\ \{\}\ \{\}$ and since $\mathsf{sim}\ \texttt{bool}\ u\ u'$ implies $u = u'$.

Proof: of Lemma. Go by induction on e.

- Case `true`: Immediate from semantic definitions.

- Case x: Immediate from semantic definitions.

- Case `if` e `then` e_1 `else` e_2: Directly by induction.

- Case `fun` $x.\ e$: Let $u = [\![D \vdash \texttt{fun}\ x.\ e : t_1 \to t_2]\!] nPh$ and let

$$u' = (\!|D \vdash \texttt{fun}\ x.\ e : t_1 \to t_2|\!) Sh'$$

Then

$$\begin{aligned} u &= \lambda P'.\ \lambda d.\ [\![D, x : t_1 \vdash e : t_2]\!] nP'[h \mid x \mapsto d] \\ u' &= \lambda S'.\ \lambda d'.\ (\!|D, x : t_1 \vdash e : t_2|\!) S'[h' \mid x \mapsto d'] \end{aligned}$$

To show $\mathsf{sim}\ (t_1 \to t_2)\ u\ u'$, need to show that for any S'', d'', d''', such that $\mathsf{sim}\ t_1\ d''\ d'''$, it is the case that $\mathsf{sim}\ t_2\ (u\ (\mathsf{privs}\ S'')\ d'')\ (u'\ S''\ d''')$. By standardness, e is `signs` $n'\ e'$ for some n', e'. Thus we can proceed as follows, using $e \equiv \texttt{signs}\ n'\ e'$ and semantics of `signs`.

$$\begin{aligned} u\ (\mathsf{privs}\ S'')\ d'' &= [\![D, x : t_1 \vdash e : t_2]\!] n\ (\mathsf{privs}\ S'')\ [h \mid x \mapsto d''] \\ &= [\![D, x : t_1 \vdash e' : t_2]\!] n'\ (\mathsf{privs}(S'') \cap \mathcal{A}(n'))\ [h \mid x \mapsto d''] \\ u'\ S''\ d''' &= (\!|D, x : t_1 \vdash e : t_2|\!)\ S''\ [h' \mid x \mapsto d'''] \\ &= (\!|D, x : t_1 \vdash e' : t_2|\!)(\langle n', \varnothing \rangle :: S'')\ [h' \mid x \mapsto d'''] \end{aligned}$$

Note that by definition sim and by assumption $\mathsf{sim}\ t_1\ d''\ d'''$, we have, $\mathsf{sim}\ (D, x : t_1)\ [h \mid x \mapsto d'']\ [h' \mid x \mapsto d''']$. Furthermore, by Fact 7.1, $\mathsf{privs}(S'') \cap \mathcal{A}(n') = \mathsf{privs}(\langle n', \varnothing \rangle :: S'')$. Therefore, by induction for e', we obtain, $\mathsf{sim}\ t_2\ (u\ (\mathsf{privs}\ S'')\ d'')\ (u'\ S''\ d''')$. This is where we need Definition 2.1.

- Case $e_1 e_2$:

$$\begin{aligned} [\![D \vdash e_1\ e_2 : t_2]\!] nPh &= \mathbf{let}\ f\ =\ [\![D \vdash e_1 : t_1 \to t_2]\!] nPh\ \mathbf{in} \\ &\quad\ \mathbf{let}\ d = [\![D \vdash e_2 : t_1]\!] nPh\ \mathbf{in}\ fPd \\ (\!|D \vdash e_1\ e_2 : t_2|\!) Sh' &= \mathbf{let}\ f'\ =\ (\!|D \vdash e_1 : t_1 \to t_2|\!) Sh'\ \mathbf{in} \\ &\quad\ \mathbf{let}\ d' = (\!|D \vdash e_2 : t_1|\!) Sh\ \mathbf{in}\ f'Sd' \end{aligned}$$

Need to show $\mathsf{sim}\ t_2\ (fPd)\ (f'Sd')$. Since $\mathsf{sim}\ D\ h\ h'$ and $P = \mathsf{privs}(S)$, therefore, by induction for e_1, we have $\mathsf{sim}\ (t_1 \to t_2)\ f\ f'$. Similarly, by induction for e_2, we have $\mathsf{sim}\ t_1\ d\ d'$. Hence the result follows by definition sim since $P = \mathsf{privs}(S)$. This case of the proof shows the necessity of defining

the relation sim.

- Case $\texttt{letrec}\ f(x) = e_1\ \texttt{in}\ e_2$:

$$\begin{aligned}
&[\![D \vdash \texttt{letrec}\ f(x) = e_1\ \texttt{in}\ e_2 : t]\!] nPh \\
&\quad = \mathbf{let}\ G(g)\ =\ \lambda P'.\ \lambda d.\ [\![D, f : t_1 \to t_2, x : t_1 \vdash e_1 : t_2]\!] nP'[h \mid f \mapsto g, x \mapsto d]\ \mathbf{in} \\
&\qquad [\![D, f : t_1 \to t_2 \vdash e_2 : t]\!] nP[h \mid f \mapsto \mathit{fix}\, G] \\
\\
&(\!|D \vdash \texttt{letrec}\ f(x) = e_1\ \texttt{in}\ e_2 : t|\!) Sh \\
&\quad = \mathbf{let}\ G'(g')\ =\ \lambda S'.\ \lambda d'.\ (\!|D, f : t_1 \to t_2, x : t_1 \vdash e_1 : t_2|\!) S'[h' \mid f \mapsto g', x \mapsto d']\ \mathbf{in} \\
&\qquad (\!|D, f : t_1 \to t_2 \vdash e_2 : t|\!) S[h' \mid f \mapsto \mathit{fix}\, G']
\end{aligned}$$

To show the result, it suffices to show $\mathsf{sim}\ (t_1 \to t_2)\ (\mathit{fix}\ G)\ (\mathit{fix}\ G')$, because then we can use induction for e_2, noting that $\mathsf{sim}\ (D, f : t_1 \to t_2)\ [h \mid f \mapsto \mathit{fix}\, G]\ [h' \mid f \mapsto \mathit{fix}\, G']$, and that $P = \mathsf{privs}(S)$. Accordingly, we demonstrate the following claim:

$$\forall i. \mathsf{sim}\ (t_1 \to t_2)\ g_i\ g'_i \tag{3}$$

Then from Lemma 7.4, we get $\mathsf{sim}\ (t_1 \to t_2)\ \bigsqcup_i g_i\ \bigsqcup_i g'_i$. This completes the proof. To show (3), we proceed by induction on i. We have:

$$\begin{aligned}
g_0 &= \lambda P'.\ \lambda d.\ \bot \\
g_{i+1} &= \lambda P'.\ \lambda d.\ [\![D, f : t_1 \to t_2, x : t_1 \vdash e_1 : t_2]\!] nP'[h \mid f \mapsto g_i, x \mapsto d] \\
&= \{\text{because } e_1 \equiv \texttt{signs}\ n'\ e'_1 \text{ by standardness}\} \\
&\quad \lambda P'.\ \lambda d.\ [\![D, f : t_1 \to t_2, x : t_1 \vdash e_1 : t_2]\!] n'(P' \cap \mathcal{A}(n'))[h \mid f \mapsto g_i, x \mapsto d] \\
\\
g'_0 &= \lambda S'.\ \lambda d'.\ \bot \\
g'_{i+1} &= \lambda S'.\ \lambda d'.\ (\!|D, f : t_1 \to t_2, x : t_1 \vdash e_1 : t_2|\!) S'[h' \mid f \mapsto g'_i, x \mapsto d'] \\
&= \{\text{because } e_1 \equiv \texttt{signs}\ n'\ e'_1\} \\
&\quad \lambda S'.\ \lambda d'.\ (\!|D, f : t_1 \to t_2, x : t_1 \vdash e'_1 : t_2|\!)(\langle n', \varnothing\rangle :: S')[h' \mid f \mapsto g'_i, x \mapsto d']
\end{aligned}$$

Clearly, $\mathsf{sim}\ (t_1 \to t_2)\ g_0\ g'_0$, by definition sim. To show $\mathsf{sim}\ (t_1 \to t_2)\ g_{i+1}\ g'_{i+1}$, assume $\mathsf{sim}\ (t_1 \to t_2)\ g_i\ g'_i$ (induction hypothesis), and that for any S' and $P' = \mathsf{privs}(S')$, $\mathsf{sim}\ t_1\ d\ d'$ holds. Then

$$\mathsf{sim}\ (D, f : t_1 \to t_2, x : t_1)\ [h \mid f \mapsto g_i, x \mapsto d]\ [h' \mid f \mapsto g'_i, x \mapsto d']$$

by definition sim and since $\mathsf{sim}\ D\ h\ h'$. Now by Fact 7.1, $P' \cap \mathcal{A}(n') = \mathsf{privs}(\langle n', \varnothing\rangle :: S')$, so by the main induction hypothesis on e'_1, $\mathsf{sim}\ t_2\ (g_{i+1} P' d)\ (g'_{i+1} S' d')$ holds.

- Case $\texttt{signs}\ n\ e$: We have: $[\![D \vdash \texttt{signs}\ n'\ e : t]\!] nPh\ =\ [\![D \vdash e : t]\!] n'(P \cap \mathcal{A}(n'))h$ and $(\!|D \vdash \texttt{signs}\ n'\ e : t|\!) Sh' = (\!|D \vdash e : t|\!)(\langle n', \varnothing\rangle :: S)h'$ so the re-

sult holds by induction on e provided $P' \cap \mathcal{A}(n') = \mathsf{privs}(\langle n', \varnothing\rangle :: S)$. But this equality holds by Fact 7.1.

- Case `dopriv` p `in` e: The result holds by induction for e, provided that $P \sqcup_n \{p\} = \mathsf{privs}(\langle n, P' \cup \{p\}\rangle :: S)$. This holds because for any p'

$$
\begin{array}{lll}
& p' \in P \sqcup_n \{p\} & \\
\Leftrightarrow & p' \in P \vee (p' \in \mathcal{A}(n) \wedge p' = p) & \text{by def } \sqcup_n \\
\Leftrightarrow & \mathsf{chk}(p', \langle n, P'\rangle :: S) \vee (p' \in \mathcal{A}(n) \wedge p' = p) & \text{assumption, def } \mathsf{privs} \\
\Leftrightarrow & (p' \in \mathcal{A}(n) \wedge (p' \in P' \vee \mathsf{chk}(p', S)) \vee (p' \in \mathcal{A}(n) \wedge p' = p) & \text{def } \mathsf{chk} \\
\Leftrightarrow & p' \in \mathcal{A}(n) \wedge (p' \in P' \cup \{p\} \vee \mathsf{chk}(p', S)) & \text{logic and sets} \\
\Leftrightarrow & p' \in \mathsf{privs}(\langle n, P' \cup \{p\}\rangle :: S) & \text{defs } \mathsf{chk} \text{ and } \mathsf{privs}
\end{array}
$$

- Case `check` p `for` e: Both semantics are conditional; the condition in one case is $p \in P'$ and in the other case $\mathsf{chk}(p, S)$, and these are equivalent conditions by assumption $P' = \mathsf{privs}(S)$ for the Lemma. In case the condition is true, the result holds by induction, which applies because for both semantics the security arguments for e are unchanged. If the condition is false, the result holds because both semantics are $\star$ and $\mathsf{sim}\ t\ \star\ \star$.

- Case `test` p `then` e_1 `else` e_2: Similar to the case for `check`.

■

8 Examples

Inspired by Skalka and Smith, we define the following standard expressions:

$$
\begin{array}{l}
lp = \texttt{fun}\ f.\ \texttt{signs}\ n\ (\texttt{fun}\ x.\ \texttt{signs}\ n\ (\texttt{dopriv}\ p\ \texttt{in}\ (f\ x))) \\
cp = \texttt{fun}\ x.\ \texttt{signs}\ n\ (\texttt{check}\ p\ \texttt{for}\ x)
\end{array}
$$

The reader can verify that one possible analysis for cp is given by the typing $\Delta;\ n \vdash cp : (\texttt{bool} \xrightarrow{\{p\}} \texttt{bool}), \varnothing.$ and that the typing demands $p \in \mathcal{A}(n)$. Similarly, the reader can verify that one possible analysis for lp is given by the typing $\Delta;\ n \vdash lp : (\texttt{bool} \xrightarrow{\{p\}} \texttt{bool}) \xrightarrow{\varnothing} (\texttt{bool} \xrightarrow{\varnothing} \texttt{bool}), \varnothing.$

For all $P \in \mathcal{P}(\mathsf{Privileges})$, for all $h : \Delta^*$, we can show (omitting types and

some steps),

$$\begin{aligned}
[\![lp]\!]nPh &= \lambda P_1.\ \lambda d_1.\ \lambda P_2.\ \lambda d_2.\ [\![\texttt{dopriv}\ p\ \texttt{in}\ f\ x]\!]n(P_2 \cap \mathcal{A}(n))[h \mid f \mapsto d_1, x \mapsto d_2] \\
&= \{\text{letting } P_3 = P_2 \cap \mathcal{A}(n)\} \\
&\quad \lambda P_1.\ \lambda d_1.\ \lambda P_2.\ \lambda d_2.\ d_1(P_3 \sqcup_n \{p\})d_2 \\
[\![cp]\!]nPh &= \lambda P_1'.\ \lambda d_1'.\ \textbf{if}\ p \in (P_1' \cap \mathcal{A}(n))\ \textbf{then}\ [\![x]\!]n(P_1' \cap \mathcal{A}(n))[h \mid x \mapsto d_1']\ \textbf{else}\ \star \\
&= \lambda P_1'.\ \lambda d_1'.\ \textbf{if}\ p \in (P_1' \cap \mathcal{A}(n))\ \textbf{then}\ d_1'\ \textbf{else}\ \star
\end{aligned}$$

Let $F = [\![lp]\!]nPh$, let $d = [\![cp]\!]nPh$ and let $G = [\![(lp\ cp)]\!]nPh$. Then

$$\begin{aligned}
[\![(lp\ cp)]\!]nPh &= FPd \\
&= \lambda P_2.\ \lambda d_2.\ \textbf{if}\ p \in ((P_3 \sqcup_n \{p\}) \cap \mathcal{A}(n))\ \textbf{then}\ d_2\ \textbf{else}\ \star \\
&= \{\text{because } p \in \mathcal{A}(n)\} \\
&\quad \lambda P_2.\ \lambda d_2.\ d_2 \\
[\![(lp\ cp)\texttt{true}]\!]nPh &= GP([\![\texttt{true}]\!]nPh) \\
&= \mathsf{true}
\end{aligned}$$

Hence $(lp\ cp)\texttt{true}$ is safe in any environment and typable as $\Delta;\ n \vdash (lp\ cp)\texttt{true} : \texttt{bool}, \varnothing$.

9 Discussion

We have given a static analysis that characterizes safe expressions, *i.e.*, ones that never cause a security violation. For such expressions, one can imagine an implementation with no security mechanism whatsoever. This seems to be the use of static analysis suggested by Skalka and Smith [4], although they do not formalize the intended implementation. On the other hand, for a language in which presence of privileges can be tested (like Java, our language, and that of Pottier *et al.* [3]), the mechanism needs to be present in some form even if some checks are eliminated. In any case, to justify the elimination of checks requires a semantic argument showing that program behavior is preserved.

It is worth recalling that the Java security model supports the principle of least privilege, which is intended in part to protect against the inevitable flaws in real implementations. It is a non-trivial engineering problem to decide how to use a static analysis; it is not necessarily desirable to eliminate all checks that could in theory be eliminated.

Program transformations give a way to describe the elimination of some, but not necessarily all, checks. Transformations may be performed selectively, at compile time and at link time. Using the eager denotational semantics, we have validated several transformations and shown their application to the password example. The applicability conditions for these particular transformations are expressed very simply, in terms of patterns using `signs` and conditions on $\mathcal{A}$. We envisage that more sophisticated transformations will depend on context conditions expressed by the static analysis. To justify such transformations, we aim to use a semantics for annotated typing judgements.

References

[1] M. Abadi, M. Burrows, B. Lampson and G. Plotkin. A calculus for access control in distributed systems. *ACM Trans. Programming Languages and Systems* 15 (4), 1993.

[2] Li Gong. *Inside Java 2 Platform Security.* Addison-Wesley, 1999.

[3] F. Pottier, C. Skalka and S. Smith. A systematic approach to static access control. *Proceedings of ESOP*, 2001.

[4] C. Skalka and S. Smith. Static enforcement of security with types. *Proceedings of the fifth ACM International Conference on Functional Programming*, 2000.

[5] D. Wallach, A. Appel and E. Felten. SAFKASI: a security mechanism for language-based systems. *ACM Trans. Software Engineering and Methodology*, 2000.