# PCAL: Language Support for Proof-Carrying Authorization Systems

Avik Chaudhuri[†] Deepak Garg

October 16, 2009
CMU-CS-09-141

School of Computer Science
Carnegie Mellon University
Pittsburgh, PA 15213

[†]Author affiliation: University of Maryland, College Park

Avik Chaudhuri was supported by DARPA under grant no. ODOD.HR00110810073. Deepak Garg was supported partially by the iCAST project sponsored by the National Science Council, Taiwan, under grant no. NSC97-2745-P-001-001, and partially by the Air Force Research Laboratory under grant no. FA87500720028. The views and conclusions contained herein are those of the authors and should not be interpreted as necessarily representing the official policies or endorsements, either expressed or implied, of the Air Force Research Laboratory, the DARPA, the U.S. Government, or Carnegie Mellon.

**Keywords:** Access control, proof-carrying authorization, language-based security

**Abstract**

By shifting the burden of proofs to the user, a proof-carrying authorization (PCA) system can automatically enforce complex access control policies. Unfortunately, managing those proofs can be a daunting task for the user. In this paper we develop a Bash-like language, PCAL, that can automate correct and efficient use of a PCA interface. Given a PCAL script, the PCAL compiler tries to statically construct the proofs required for executing the commands in the script, while re-using proofs to the extent possible and rewriting the script to construct the remaining proofs dynamically. We obtain a formal guarantee that if the policy does not change between compile time and run time, then the compiled script cannot fail due to access checks at run time.

# 1 Introduction

Proof-carrying authorization (PCA) [3,5,6,18,20,22] is a modern access control technology, where an access control policy is formalized as a set of *logical formulas*, and a principal is allowed to perform an operation on a resource only if that principal can produce a *proof* showing that the policy *entails* that the principal may perform the operation on the resource. While this architecture allows automatic enforcement of complex access control policies, it substantially increases the burden of the user, since each request to perform an operation must be accompanied by one or more proofs. Furthermore, even if the user employs a theorem prover to construct the proofs, the user must still ensure that enough proofs are generated for each request to succeed, while minimizing the costs of proof construction at run time. In this paper we develop a programming language that can assist the user in performing such tasks correctly and automatically in a system with PCA. We have implemented a compiler for our language and tested it with a PCA-based file system, PCFS [18].

Our language, PCAL, extends the Bash scripting language with some PCA-specific annotations; the PCAL compiler translates programs with these annotations to ordinary Bash scripts, to be executed in a system with PCA. More precisely, PCAL annotations can specify what proofs the programmer expects to hold at particular program points. Based on these annotations, the compiler performs the following tasks.

1. It checks that the programmer's expectations about proofs suffice to allow successful execution of every shell command in the script. For this, the compiler needs to know what permissions are required to execute each shell command. We provide this information through a configuration file.

2. Next, the compiler uses a theorem prover and information about the access control policy to try to *statically* construct proofs corresponding to the programmer's annotations. In cases where static proof construction fails, because the annotations do not convey enough static information, the compiler generates code that constructs the proof at run time by calling the theorem prover from the command line.

3. Finally, the compiler adds code to pass appropriate proofs for each shell command to the PCA interface.

Thus, the output of the compiler is a Bash script which, beyond the usual commands, contains some code to generate proofs at run time (when it cannot generate such proofs at compile time), and some code to pass the proofs, generated either statically or dynamically, to the PCA interface.

Using PCAL offers at least two advantages over a naive approach, where a user generates and passes to the PCA interface enough proofs of access before running an unannotated script.

1. Because of the static checks and dynamic code generated by the compiler, it is guaranteed that the resulting script will *at least try to construct all necessary proofs of*

*access*. Thus, the script can fail only if the user does not have enough privileges to run it, and not because the user forgot to create some proofs. Indeed, we formally prove that if compilation of a program succeeds and the policy does not change between compilation and program execution, then the program cannot fail due to an access check (Theorem 4.2). This is very significant for scripts where the user cannot determine a priori what operations the script will perform.

2. Since the compiler sees all commands that the script will execute, it re-uses proofs to the extent possible and reduces the proof construction overhead, which a naive user may not be able to do. This is particularly relevant for POSIX-like policies where accessing a file requires an "execute" permission on all its ancestor directories. If several files in a directory need to be processed, there is no need to construct proofs for the ancestor directories again and again. The PCAL compiler takes advantage of this and other similar structure in policies and combines it with information about a program's commands to minimize proof construction.

By design, PCAL and its compiler are largely independent of the logic used to express policies. The compiler requires a theorem prover compatible with the logic used, but it does not analyze formulas or proofs itself. Thus, the compiler can be (trivially) modified to use a different logic. Similarly, the compiler is parametric in the shell commands it supports. It assumes a map from each shell command to the permissions needed to execute it, and a single command to pass proofs to the PCA interface. By replacing this map and the command, the compiler can be used to support any PCA interface, not necessarily a file system.

PCAL is distinct from other work that combines PCA with a programming language [4, 20]. In all such prior work, the language is used to enforce access control statically. On the other hand, PCAL uses a *combination* of static checks and dynamic code to ensure compliance with the requirements of the PCA interface. Static enforcement is a special case of this approach, where an input program is rejected unless the compiler can construct all required proofs at compile time. Furthermore, in all prior work proofs are data or type structures and programmers must write explicit code to construct them. In particular, programmers must understand the logic. In contrast, PCAL separates proofs from programs, and shifts the burden of constructing proofs (and understanding the logic) from programmers to an automatic theorem prover. We believe that this not only makes PCAL's design modular, but also easier to use.

### Contributions

We believe that we are the first to propose, design, and implement a language that uses a combination of static checks and dynamic code to optimize the proof burden of a PCA-compliant program. This setting presents some unique technical challenges, and our design and implementation require some novel elements to deal with those challenges.

1. While we would like to discharge as many proofs as possible statically, we must be concerned about possibly invalidating the assumptions underlying those proofs at run

time. For instance, the state of the system may not remain invariant between compile time and run time. This requires a careful separation of (dynamic) state conditions from other (static) policies.

2. Since the values of some program variables cannot be determined at compile time, the PCAL compiler constructs *quantified proofs* which are parametric over these program variables. These variables are substituted at run time to obtain ground proofs. (See Section 5 for details.)

3. Programmer annotations in PCAL have both static and dynamic semantics. Statically, they *specify* authorization conditions and other constraints that should hold at run time, thereby aiding verification of correctness by the compiler. Dynamically, they *verify* any assumptions on the existence of authorization proofs and other constraints made by the compiler, thereby allowing sound optimizations.

4. For practical reasons, we must also be concerned about balancing the relative strengths and weaknesses of a theorem prover (to discharge proofs) and compiler (to analyze programs). We achieve such a balance by working at several levels of abstraction. While all functions and predicates used in a script have concrete implementations at run time, the compiler only partially interprets these functions and predicates with abstract rewrite rules, so that the program can be analyzed with appropriate precision by symbolic techniques. Furthermore, calls to the theorem prover are simplified, so that the theorem prover can treat all functions and predicates as uninterpreted, and thus can search for proofs efficiently. Tying these levels of abstraction together requires some care in the implementation. This is discussed further in Section 5.

5. We prove formally that the behavior of a compiled program is the same as that of the source program (Theorem 4.1) and that successfully compiled programs cannot fail due to access checks (Theorem 4.2). The proofs of these theorems require a precise characterization of assumptions on the theorem prover, the proof verifier, and the relation between the environment in which the program is compiled and that in which it is executed. We believe that this characterization is a significant contribution of this work, because it is fundamental to any architecture that uses a similar approach.

The rest of the paper is organized as follows. After closing this section with a brief review of related work, in Section 2 we discuss some background material covering PCA, and the assumptions we make about the interface it provides. Section 3 introduces PCAL and its compiler through an example. Details of the language, its compilation, and correctness theorems are covered in Section 4. Some important implementation-related issues are discussed in Section 5.

### Related Work

There are two prior lines of work on combining proofs of authorization with languages. The first line of work includes the languages Aura [20, 24] and $\text{PCML}_5$ [4], where PCA as well

as a logic for expressing policies are embedded in the type system, and proofs are data or type structures that programs can analyze. This contrasts with PCAL, where proofs cannot be analyzed. PCAL's approach is advantageous because it decouples the logic from the language, thus making it easy to use the same compiler with different logics. It also alleviates the programmer's burden of understanding the logic. On the other hand, in Aura and $\text{PCML}_5$, parts of proofs can be re-used in different places, thus allowing potentially more efficient proof construction than in PCAL. However, it is unclear whether this advantage extends when automatic theorem provers are used in either Aura or $\text{PCML}_5$.

The second line of work includes several languages that culminate in the most recent F7 [8, 14]. These languages use an external logic like PCAL, but the objective is to express logical conditions. The programmer can introduce logical assumptions at different program points, and check statically at other program points that those assumptions entail some other formula(s). In PCAL it is not necessary that each programmer annotation about a proof succeed statically; if it fails, code to construct the proof at run time is automatically inserted. This approach is similar to hybrid typechecking [13], especially as applied to recent security type systems [9, 11]. Indeed, PCAL departs from previous lines of work in that it does not try to enforce security on its own; instead it is meant as a tool to help programs comply with a PCA interface that enforces security.

PCA, the architecture that PCAL supports, was introduced by Appel and Felten [3]. It has been applied in different settings including authorization for web services [5], the Grey system [6], and the file system PCFS [18]. The latter implementation is the basic test bench for PCAL. The specific logic used for writing policies in this paper (and PCFS) is BL [15, 16]. It is related to, but more expressive than, many other logics and languages for writing access policies (*e.g.*, [1, 2, 7, 12, 17, 19, 23]).

## 2 Background

In this section we provide a brief overview of PCA, and list particular assumptions that PCAL makes about the underlying PCA-based system interface.

PCA [3, 5, 6, 18, 20, 22] is a general architecture for enforcing access control in settings that require complex, rule-based policies. Policy rules are expressed as formulas in some fixed logic, and enforced automatically using formal proofs. Let $\mathcal{L}$ denote a set of formulas that represent the access policy (see Section 3 for an example). The system interface grants user $A$ permission $\eta$ (*e.g.*, read, write) on a resource $t$ (*e.g.*, a file) only if $A$ produces a formal proof $\gamma$ which shows that $\mathcal{L}$ entails a formula $\mathbf{auth}(A, \eta, t)$ in the logic's proof system. The formula $\mathbf{auth}(A, \eta, t)$ means that $A$ has permission $\eta$ on resource $t$. Its exact form depends on the logic in use and the resources being protected, but is irrelevant for the purposes of this paper. (Here it suffices to assume that $\mathbf{auth}(A, \eta, t)$ is an atomic formula.) The system interface checks the proof that $A$ provides to make sure that it uses the logic's inference rules correctly, and that it proves the intended formula. The system interface must provide a mechanism by which users can submit proofs either prior to or along with an access request. Even though users are free to construct proofs by any means they like,

it is convenient to have an automatic theorem prover to perform this task.

**Assumptions**

PCAL's compiler supports rich logics for writing policies, in which proofs may depend not only on the formulas constituting the policy, but also on system state (*e.g.*, meta-data of files and clock time). Let $H$ denote the system state. We write $\gamma :: H; \mathcal{L} \vdash s$ to mean that $\gamma$ is a formal proof which shows that in the system state $H$, policies $\mathcal{L}$ entail formula $s$. (In particular, $s$ may be $\mathbf{auth}(A, \eta, t)$.)

PCAL assumes that an automatic theorem prover for the logic is available, both through an API and as a command line tool. A call to the theorem prover (either through the API or the command line) is formally summarized by the notation $H; \mathcal{L} \vdash s \searrow \gamma$, which means that asking the theorem prover to construct a proof for $s$ from policy $\mathcal{L}$ in state $H$ results in the proof $\gamma$. Dually, $H; \mathcal{L} \vdash s \not\searrow$ means that the theorem prover fails to construct a corresponding proof. The latter *does not* imply the absence of a proof in the logic, since the theorem prover may implement an incomplete search procedure. The following command is assumed to invoke the prover from the command line and store in the file `pf` a proof which establishes $\mathbf{auth}(A, \eta, t)$ from the policies in `/pl` and the prevailing system state.

`prove` $\mathbf{auth}(A, \eta, t)$ `/pl > pf`

For passing proofs to the system interface, we assume a simple protocol: a command `inject` is called from the command line to give a proof to the system interface, which puts it in a store that is indexed by the triple $(A, \eta, t)$ authorized by the proof. During the invocation of a system API, relevant proofs are retrieved from this store and checked. For example, the following command injects the proof in the file `pf` into the interface's store.

```
inject pf
```

While proofs required to execute commands at run time must be ground, proofs produced at compile time may contain free variables, which we assume are listed in order, and which need to be instantiated at run time. For such proofs, the run-time substitutions of such variables are also provided to the `inject` command (with option `-subst`), so that the injected proofs are always ground. For example, the following command substitutes the run-time values of some Bash variables (in order) for the free variables in the proof read from file `.pf` and stores the resulting proof in the system interface.

```
inject pf -subst $_PRIN $z $x $y $bar $foo
```

# 3 Overview of PCAL

In this section, we work through a small example to demonstrate the steps of our compilation. (PCAL is formalized in Section 4.) For this example, let there be a predicate `extension` and functions `path` and `base`, such that (informally):

- `extension`$(f, e)$ holds if file $f$ has extension $e$;
- `path`$(d, x) = p$ if path $p$ is the concatenation of directory $d$ and name $x$;
- `base`$(p) = x$ if `path`$(d, x) = p$ for some directory $d$.

Consider the program $P$ in Figure 1, written in PCAL. This program iterates through the files in some directory `foo` (unspecified), copying them to a directory `bar` (set to `"/tmp"`). Furthermore, it touches those files in `foo` that have extension `"log"`. The reader may ignore the `assert` statements (in lines 2, 8, 12, and 13) in a first reading; we explain their meaning below.

The system is configured to check, for any command, that certain permissions are held on certain paths in order to execute that command. Let us assume the following configuration:

**Configuration**

- Iterating over directory $d$ requires permission `read` on $d$.
- Executing the shell command `touch`$(f)$ requires permission `write` on file $f$.
- Executing the shell command `cp`$(f_1, f_2)$ requires permission `read` on file $f_1$, and permission `write` on file $f_2$.

The `assert` statements in $P$ serve to establish, at run time, that the principal running the script has particular permissions on particular paths. The compiler tries to statically identify `assert` statements that must succeed at run time, and eliminate them at compile time.

Assume that `member` is a predicate such that `member`$(f, d)$ holds if file $f$ is in directory $d$. Consider the following policy, written in a first-order logic with the convention that implication $\Rightarrow$ is right associative.

**Policy**

$$\begin{aligned}
&\textbf{auth}(\texttt{"User"}, \texttt{read}, \texttt{"/home"}).\\
&\forall A.\forall x.\ \textbf{auth}(A, \texttt{write}, \texttt{path("/tmp", x)}).\\
&\forall A.\forall x.\forall y.\ \texttt{member}(x, y) \Rightarrow \textbf{auth}(A, \texttt{read}, y) \Rightarrow\\
&\qquad\qquad (\textbf{auth}(A, \texttt{read}, x) \wedge\\
&\qquad\qquad (\texttt{extension}(x, \texttt{"log"}) \Rightarrow \textbf{auth}(A, \texttt{write}, x))).
\end{aligned}$$

Informally, the policy asserts the following:

- the principal `"User"` has permission `read` on directory `"/home"`
- any principal $A$ has permission `write` on any file in the directory `"/tmp"`

Program $P$

```
 1 bar = "/tmp";
 2 assert (read, foo);
 3 for x in foo {
 4     y = x;
 5     x = base(x);
 6     z = path(foo, x);
 7     test extension(z, "log") {
 8          assert (write, z);
 9          shell touch(z)
10     };
11     z = path(bar, x);
12     assert (write, z);
13     assert (read, y);
14     shell cp(y, z)
15 }
```

Program $Q$

```
 1 bar = "/tmp";
 2 assert (read, foo);
 3 for x in foo {
 4     y = x;
 5     x = base(x);
 6     z = path(foo, x);
 7     test extension(z, "log") {
 8          -- assert (write, z);
 9          shell touch(z)
10     };
11     z = path(bar, x);
12     -- assert (write, z);
13     -- assert (read, y);
14     shell cp(y, z)
15 }
```

Script $\mathcal{S}$

```
  !/bin/bash
  function base { _RET=${1##*/} }
  function path { _RET=$1/$2 }
  function extension { if [ ${1##*.} = $2 ]; then _RET="ok"; fi }
  _PRIN="User"
  foo="/home"

 1 bar="/tmp"
 2 prove auth ($_PRIN, read, $foo) /pl > pf
   inject pf
 3 for x in `ls $foo`; do x=$foo/$x
 4   y=$x
 5   _RET="_"; base $x; x=$_RET
 6   _RET="_"; path $foo $x; z=$_RET
 7   _RET="_"; extension $z "log"; if [ $_RET = "ok" ]; then
 8     inject /pf/1 -subst $_PRIN $z $x $y $bar $foo
 9     touch $z
10   fi
11   _RET="_"; path $bar $x; z=$_RET
12   inject /pf/2 -subst $_PRIN $z $x $y $bar $foo
13   inject /pf/3 -subst $_PRIN $z $x $y $bar $foo
14   cp $y $z
15 done
```

Figure 1: Translation of an input program $P$, via an intermediate program $Q$, to an output script $\mathcal{S}$. (The configuration, policy, and rewrite theory provided to the compiler are shown elsewhere.)

- for any principal $A$, file $x$, and directory $y$, if $x$ is in $y$ and $A$ has permission `read` on $y$, then $A$ has permission `read` on $x$, and furthermore, if $x$ has extension `"log"` then $A$ has permission `write` on $x$.

Finally, consider the following theory on the function symbols `path` and `base`, that abstracts the concrete semantics of these functions.

**Theory**

$$\forall x.\forall y.\ \texttt{member}(x, y) \Rightarrow \texttt{path}(y, \texttt{base}(x)) = x$$

Given the configuration, policy, and theory above, our compiler automatically translates $P$ to the intermediate program $Q$ in Figure 1. In $Q$, all `assert` statements except that in line 2 are eliminated, since the compiler can infer that they must succeed at run time. Such inference requires collection of path conditions, partial evaluation of terms modulo the given equational theory, and calls to the theorem prover. We describe the compiler in detail in Sections 4 and 5.

In particular, for the `assert` statement in line 8, the compiler reasons automatically as follows. Let `_PRIN` be the principal running the script. Line 8 is reached only if the following conditions hold for some `z`, `x`, $x'$, and `foo`:

(1) `extension(z, "log")`.

(2) `z` = `path(foo, x)`.

(3) `x` = `base`($x'$).

(4) `member`($x'$, `foo`).

(5) The statement `assert (read, foo)` in line 2 succeeds.

From condition (5), we can conclude that

(6) **auth**(`_PRIN`, `read`, `foo`).

Simplifying conditions (2), (3), and (4) using the given theory, we have

(7) `z` = $x'$.

Now from conditions (1), (4), (6), and (7) and the given policy, the theorem prover can conclude that **auth**(`_PRIN`, `write`, $z$), which is sufficient to eliminate the `assert` statement in line 8.

Next, we want to be able to run the intermediate program $Q$ on a file system that supports PCA. The compiler translates $Q$ to the equivalent Bash script $\mathcal{S}$ in Figure 1. The commands `prove` and `inject` perform functions described in Section 2. The header (the part of $\mathcal{S}$ before the numbered lines) defines all free variables (`_PRIN` and `foo`) and uninterpreted functions and predicates (`path`, `base`, `extension`) in $P$. The implementations

of such functions and predicates are sound with respect to the equational theory used by the compiler.

We close this section by discussing our trust assumptions. A policy is trusted, so any interpreted predicates in a policy (such as `member` and `extension`) must have trusted implementations (provided by the system). In contrast, a program is not trusted. The compiler may or may not be trusted. If the compiler is trusted, then the system can trust scripts produced by the compiler, and run such scripts without checking the proofs that they inject. This is significant in implementations where proofs may be large and proof verification may be costly. However, such a compiler cannot assume semantic properties of the functions used in a program (such as `base` and `path`) unless those functions have trusted implementations that are provided by the system. On the other hand, if the compiler is not trusted then the system must run all scripts with access checks. We implicitly assume the latter scenario in the sequel, and provide additional guarantees for the scenario in which the compiler is trusted (Theorem 4.2).

# 4 PCAL: Syntax, Semantics, and Compilation

We now describe the PCAL language and its compiler. We present the syntax of PCAL programs, define their operational semantics, formalize our compilation procedure and show that it preserves the behavior of programs.

For simplicity of presentation, we abstract various details of the implementation. (See Section 5 for a more detailed discussion.) Instead of Bash, we consider an extension of PCAL as the target language for compilation; programs in this target language can be easily rewritten to Bash. We also treat all function symbols as uninterpreted, although in principle, equations over terms may be freely added in the run time semantics (to model concrete implementations) and in the compiler (to model abstract properties of such implementations).

We assume that $\eta$, $x$, and $t$ range over permissions, variables, and terms whose grammars are borrowed from the logic used to represent policies. $\varphi$ denotes a logical predicate whose truth depends only on the system state (*i.e.*, a predicate that is not defined by logical rules). PCAL programs are sequences of statements $e$ described by the grammar below. Directories, files, and paths are represented as terms, and $\chi$ is a special variable that is bound to the principal running a program.

**Syntax**

| | |
|---|---|
| $e ::=$ | statements |
| $\mathsf{for}\ x\ \mathsf{in}\ t\ \{P\}$ | for each file $f$ in directory $t$, bind $x$ to $f$ and do $P$ |
| $\mathsf{test}\ \varphi\ \{P\}$ | if condition $\varphi$ holds, do $P$ |
| $x = t$ | assign $t$ to $x$ |
| $\mathsf{shell}\ n(t_1, \ldots, t_k)$ | call shell command $n$ with parameters $t_1, \ldots, t_k$ |
| $\mathsf{assert}\ (\eta, t)$ | assert that principal $\chi$ has permission $\eta$ on path $t$ |
| $P, Q ::=$ | programs |

| | |
|---|---|
| $e; Q$ | run $e$, then do $Q$ |
| $\mathsf{end}$ | skip/halt |

We also consider below an extension of PCAL which acts as the target language for the compiler. $\alpha = \mathsf{prove}\ (\eta, t)$ and $\mathsf{inject}\ (\eta, t)\ \gamma$ are formal representations of the commands `prove` and `inject` from Section 2. $\gamma$ ranges over proofs and $\alpha$ denotes a variable bound to a proof (which, in the actual implementation, is a temporary file that stores the proof; see Section 5).

**Extended syntax**

| $e ::=$ | statements |
|---|---|
| ... | |
| $\alpha = \mathsf{prove}\ (\eta, t)$ | prove that principal $\chi$ has permission $\eta$ on path $t$ and bind the proof to $\alpha$ |
| $\mathsf{inject}\ (\eta, t)\ \gamma$ | inject proof $\gamma$ that authorizes $(\chi, \eta, t)$ |

**Semantics**

A PCAL program runs in an environment $\theta$ of the form $(\Delta, \mathcal{L})$, where $\Delta$ is a function from shell command names to lists of permissions (configuration) and $\mathcal{L}$ is the set of logical formulas used to determine access (policy). Informally, if $\Delta(n) = \eta_1, \ldots, \eta_k$ then executing shell command $n(t_1, \ldots, t_k)$ requires permissions $\eta_1, \ldots, \eta_k$ on paths $t_1, \ldots, t_k$ respectively.

A state $\rho$ is a triple $(H, S, \xi)$, where $H$ is an abstract, logical representation of the part of the system state on which proofs of access depend, $S$ is a function from paths to terms (data store), and $\xi$ is a partial function from triples $(A, \eta, t)$ to proofs (proof store). $H$ must contain, at the least, information about members of directories. We write $\texttt{members}(H, t)$ to denote the list of files in directory $t$ in the system state $H$. Proofs injected using $\mathsf{inject}\ (\eta, t)\ \gamma$ are added to $\xi$.

Reductions are of the form $\rho, P \xrightarrow{\theta, \chi} \rho', P'$, meaning that program $P$ at state $\rho$, run by principal $\chi$ in environment $\theta$, reduces to program $P'$ at state $\rho'$. The reduction rules are shown in Figure 2. $H, S \overset{n(t_1, \ldots, t_k)}{\blacktriangleright} H', S'$ means that executing the shell command $n(t_1, \ldots, t_k)$ updates the system state $H$ and data store $S$ to $H'$ and $S'$ respectively. $H \models \varphi$ means that $\varphi$ holds in $H$, and $H \not\models \varphi$ means that $\varphi$ does not hold in $H$. In practice, whether $\varphi$ holds in $H$ or not is decided using a trusted decision procedure provided by the system.

- **(Reduct for)** unrolls a loop $P$ for each file $x$ in a directory $t$. **(Reduct test)** simplifies $\mathsf{test}\ \varphi\ \{P\}; Q$ to $P; Q$ if $H \models \varphi$, and to $Q$ otherwise. **(Reduct assign)** is straightforward.
- **(Reduct shell)** finds proofs $\gamma_1, \ldots, \gamma_n$ needed to authorize the shell command $n(t_1, \ldots, t_k)$ in the proof store $\xi$. It then checks these proofs (premise $\gamma_i :: H; \mathcal{L} \vdash \mathbf{auth}(\chi, \eta_i, t_i)$), and executes the shell command (premise $H, S \overset{n(t_1, \ldots, t_k)}{\blacktriangleright} H', S'$).

**Reduction** $\rho, P \xrightarrow{\theta,\chi} \rho', P'$

**(Reduct for)**
$$\frac{\rho = (H, \_, \_) \qquad \texttt{members}(H, t) = t_1, \ldots, t_k}{\rho, \mathsf{for}\ x\ \mathsf{in}\ t\ \{P\}; Q \xrightarrow{\theta,\chi} \rho, P\{t_1/x\}; \ldots; P\{t_k/x\}; Q}$$

**(Reduct test)**
$$\frac{\rho = (H, \_, \_) \qquad H \vDash \varphi}{\rho, \mathsf{test}\ \varphi\ \{P\}; Q \xrightarrow{\theta,\chi} \rho, P; Q} \qquad \frac{\rho = (H, \_, \_) \qquad H \nvDash \varphi}{\rho, \mathsf{test}\ \varphi\ \{P\}; Q \xrightarrow{\theta,\chi} \rho, Q}$$

**(Reduct assign)**
$$\rho, x = t; Q \xrightarrow{\theta,\chi} \rho, Q\{t/x\}$$

**(Reduct shell)**
$$\frac{\begin{array}{c}\theta = (\Delta, \mathcal{L}) \qquad \Delta(n) = \eta_1, \ldots, \eta_k \qquad \rho = (H, S, \xi) \\ \xi(\chi, \eta_i, t_i) = \gamma_i \qquad \gamma_i :: H; \mathcal{L} \vdash \mathbf{auth}(\chi, \eta_i, t_i) \\ H, S \overset{n(t_1,\ldots,t_k)}{\blacktriangleright} H', S' \qquad \rho' = (H', S', \xi)\end{array}}{\rho, \mathsf{shell}\ n(t_1, \ldots, t_k); P \xrightarrow{\theta,\chi} \rho', P}$$

**(Reduct assert)**
$$\frac{\begin{array}{c}\theta = (\_, \mathcal{L}) \qquad \rho = (H, S, \xi) \\ H; \mathcal{L} \vdash \mathbf{auth}(\chi, \eta, t) \searrow \gamma \qquad \rho' = (H, S, \xi[(\chi, \eta, t) \mapsto \gamma])\end{array}}{\rho, \mathsf{assert}\ (\eta, t); P \xrightarrow{\theta,\chi} \rho', P}$$

**(Reduct prove)**
$$\frac{\theta = (\_, \mathcal{L}) \qquad \rho = (H, \_, \_) \qquad H; \mathcal{L} \vdash \mathbf{auth}(\chi, \eta, t) \searrow \gamma}{\rho, \alpha = \mathsf{prove}\ (\eta, t); P \xrightarrow{\theta,\chi} \rho, P\{\gamma/\alpha\}}$$

**(Reduct inject)**
$$\frac{\rho = (H, S, \xi) \qquad \rho' = (H, S, \xi[(\chi, \eta, t) \mapsto \gamma])}{\rho, \mathsf{inject}\ (\eta, t)\ \gamma; P \xrightarrow{\theta,\chi} \rho', P}$$

Figure 2: Reduction rules

- **(Reduct assert)** calls the theorem prover to construct a proof $\gamma$ which shows that $\chi$ has permission $\eta$ on path $t$ (premise $H; \mathcal{L} \vdash \mathbf{auth}(\chi, \eta, t) \searrow \gamma$), and passes it to the system interface by placing it in the store $\xi$.
- **(Reduct prove)** constructs a proof $\gamma$ and binds $\alpha$ to it. **(Reduct inject)** places a proof $\gamma$ in the proof store $\xi$. By these rules, the effect of the command sequence $\alpha = \mathsf{prove}\ (\eta, t); \mathsf{inject}\ (\eta, t)\ \alpha$ is exactly the same as the command $\mathsf{assert}\ (\eta, t)$. However, $\mathsf{assert}\ (\eta, t)$ occurs only in source programs whereas $\mathsf{prove}\ (\eta, t)$ and $\mathsf{inject}\ (\eta, t)\ \gamma$ occur only in compiled programs.

### Compilation

Next, we formalize compilation of PCAL programs. As the compiler traverses a program, it maintains a database of facts that must be true at the program point that the compiler

is looking at. These facts are formally represented by $\Gamma = (\sigma, \Phi, \Xi)$.

- $\sigma$ is a list of substitutions of the form $\{t/x\}$. The latter means that program variable $x$ is bound to term $t$.
- $\Phi$ is a list of interpreted predicates $\varphi$ that can be assumed to hold at a program point. These are gathered from commands $\mathsf{test}\ \varphi\ \{\ldots\}$ and $\mathsf{for}\ x\ \mathsf{in}\ t\ \{\ldots\}$. In particular, $\varphi$ may be of the form $\texttt{member}(t', t)$, meaning that path $t'$ is in directory $t$; and we assume that $\texttt{members}(H, t) = t_1, \ldots, t_k$ implies $H \vDash \texttt{member}(t_1, t) \wedge \cdots \wedge \texttt{member}(t_k, t)$.
- $\Xi$ is a partial function from triples $(A, \eta, t)$ to authorization proofs that the compiler has already constructed.

Figure 3 shows the rules to derive judgments of the form $\Gamma \vdash P \overset{H,\theta,\chi}{\rightsquigarrow} P'$, meaning that under assumptions $\Gamma$, program $P$ compiles to program $P'$ in environment $\theta$ and system state $H$. $\chi$ is given to the compiler at the time of invocation; it represents the user who is expected to run the compiled program. $H$ is the state of the system in which the compiled program is expected to run. It may either be the system state at the time of compilation (if it is expected that the compiled program will run in the same state), or it may be a state that the user provides. Both $\chi$ and $H$ are needed to call the theorem prover during compilation.

For any syntactic entity $\mathbb{E}$, we write $\mathbb{E}\sigma$ to denote the result of applying the substitution $\sigma$ to $\mathbb{E}$. $\mathcal{W}(P)$ denotes the variables that are assigned in the program $P$, and $\sigma\backslash\widetilde{x}$ denotes the restriction of $\sigma$ that removes the mappings for all variables in $\widetilde{x}$. Finally, $|\Xi|$ and $\langle\Xi\rangle$ extract the formulas and proofs in $\Xi$ ($\prod$ denotes tupling of proofs):

$$|\Xi| = \bigwedge_{(A,\eta,t)\in\mathsf{dom}(\Xi)} \mathbf{auth}(A, \eta, t) \qquad \langle\Xi\rangle = \prod_{\gamma\in\mathsf{rng}(\Xi)} \gamma$$

- **(Comp end)** terminates compilation when $\mathsf{end}$ is seen.
- **(Comp for)** compiles $\mathsf{for}\ x\ \mathsf{in}\ t\ \{P\}; Q$ by compiling $P$ to $P'$ under the added assumption $\texttt{member}(x, t\sigma)$ (which must hold inside the body of the loop), and compiling $Q$ to $Q'$. In each case, any prior substitutions for variables $\widetilde{x}$ assigned in $P$ are removed from $\sigma$, because they may be invalidated during the execution of the loop (premises $\widetilde{x} = \mathcal{W}(P)$ and $\sigma' = \sigma\backslash\widetilde{x}$).
- **(Comp test)** is similar to **(Comp for)**; in this case the assumption $\varphi\sigma$ is added when compiling the body $P$ of the test branch.
- **(Comp assign)** records the effect of assignment $x = t$ by augmenting substitution $\sigma$ with $\{t\sigma/x\}$. This augmented substitution is used to compile the remaining program.
- **(Comp shell)** checks that there is a proof in the set of previously constructed proofs $\Xi$ to authorize each permission needed to execute a shell command $n(t_1, \ldots, t_k)$. (Proofs are added to this set in the next two rules).

**Compilation** $\Gamma \vdash P \overset{H,\theta,\chi}{\rightsquigarrow} P'$

**(Comp end)**
$$\Gamma \vdash \mathsf{end} \overset{H,\theta,\chi}{\rightsquigarrow} \mathsf{end}$$

**(Comp for)**
$$\frac{\begin{array}{c}\Gamma = (\sigma, \Phi, \Xi) \qquad \widetilde{x} = \mathcal{W}(P) \qquad \sigma' = \sigma\backslash\widetilde{x} \\ x \text{ fresh in } \Gamma \qquad \Phi' = \Phi, \mathtt{member}(x, t\sigma) \\ (\sigma', \Phi', \Xi) \vdash P \overset{H,\theta,\chi}{\rightsquigarrow} P' \qquad (\sigma', \Phi, \Xi) \vdash Q \overset{H,\theta,\chi}{\rightsquigarrow} Q'\end{array}}{\Gamma \vdash \mathsf{for}\ x\ \mathsf{in}\ t\ \{P\}; Q \overset{H,\theta,\chi}{\rightsquigarrow} \mathsf{for}\ x\ \mathsf{in}\ t\ \{P'\}; Q'}$$

**(Comp test)**
$$\frac{\begin{array}{c}\Gamma = (\sigma, \Phi, \Xi) \qquad \widetilde{x} = \mathcal{W}(P) \qquad \sigma' = \sigma\backslash\widetilde{x} \qquad \Phi' = \Phi, \varphi\sigma \\ (\sigma, \Phi', \Xi) \vdash P \overset{H,\theta,\chi}{\rightsquigarrow} P' \qquad (\sigma', \Phi, \Xi) \vdash Q \overset{H,\theta,\chi}{\rightsquigarrow} Q'\end{array}}{\Gamma \vdash \mathsf{test}\ \varphi\ \{P\}; Q \overset{H,\theta,\chi}{\rightsquigarrow} \mathsf{test}\ \varphi\ \{P'\}; Q'}$$

**(Comp assign)**
$$\frac{\Gamma = (\sigma, \Phi, \Xi) \qquad \sigma' = \sigma[x \mapsto t\sigma] \qquad (\sigma', \Phi, \Xi) \vdash P \overset{H,\theta,\chi}{\rightsquigarrow} P'}{\Gamma \vdash x = t; P \overset{H,\theta,\chi}{\rightsquigarrow} x = t; P'}$$

**(Comp shell)**
$$\frac{\begin{array}{c}\theta = (\Delta, \_) \qquad \Delta(n) = \eta_1, \ldots, \eta_k \qquad \Gamma = (\sigma, \_, \Xi) \\ (\chi, \eta_i, t_i\sigma) \in \mathsf{dom}(\Xi) \text{ for each } i \qquad \Gamma \vdash P \overset{H,\theta,\chi}{\rightsquigarrow} P'\end{array}}{\Gamma \vdash \mathsf{shell}\ n(t_1, \ldots, t_k); P \overset{H,\theta,\chi}{\rightsquigarrow} \mathsf{shell}\ n(t_1, \ldots, t_k); P'}$$

**(Comp static)**
$$\frac{\begin{array}{c}\Gamma = (\sigma, \Phi, \Xi) \qquad \theta = (\_, \mathcal{L}) \\ H, \Phi; \mathcal{L} \vdash |\Xi| \Rightarrow \mathbf{auth}(\chi, \eta, t\sigma) \searrow \gamma' \qquad \gamma = \gamma'\ \langle\Xi\rangle \\ \Xi' = \Xi[(\chi, \eta, t\sigma) \mapsto \gamma] \qquad \Gamma' = (\sigma, \Phi, \Xi') \qquad \Gamma' \vdash P \overset{H,\theta,\chi}{\rightsquigarrow} P'\end{array}}{\Gamma \vdash \mathsf{assert}\ (\eta, t); P \overset{H,\theta,\chi}{\rightsquigarrow} \mathsf{inject}\ (\eta, t)\ \gamma; P'}$$

**(Comp dynamic)**
$$\frac{\begin{array}{c}\Gamma = (\sigma, \Phi, \Xi) \qquad \theta = (\_, \mathcal{L}) \\ H, \Phi; \mathcal{L} \vdash |\Xi| \Rightarrow \mathbf{auth}(\chi, \eta, t\sigma) \not\searrow \qquad \alpha \text{ fresh in } \Gamma, P \\ \Xi' = \Xi[(\chi, \eta, t\sigma) \mapsto \alpha] \qquad \Gamma' = (\sigma, \Phi, \Xi') \qquad \Gamma' \vdash P \overset{H,\theta,\chi}{\rightsquigarrow} P'\end{array}}{\Gamma \vdash \mathsf{assert}\ (\eta, t); P \overset{H,\theta,\chi}{\rightsquigarrow} \alpha = \mathsf{prove}\ (\eta, t); \mathsf{inject}\ (\eta, t)\ \alpha; P'}$$

Figure 3: Compilation rules

- **(Comp static)** and **(Comp dynamic)** are used to compile the command $\mathsf{assert}\ (\eta, t)$ in different cases. To decide which rule to use, the compiler tries to statically prove $|\Xi| \Rightarrow \mathbf{auth}(\chi, \eta, t\sigma)$ by calling the theorem prover. The context in which the proof is constructed not only contains $H$ and the policy $\mathcal{L}$, but also information about directory memberships and predicates tested in outer scopes ($\Phi\sigma$). If a proof $\gamma'$ can be constructed, rule **(Comp static)** is used: $\mathsf{assert}\ (\eta, t)$ is replaced by $\mathsf{inject}\ (\eta, t)\ \gamma$, which passes the statically generated proof $\gamma = \gamma'\ \langle\Xi\rangle$ to the system interface at run

time. ($\gamma'$ $\langle\Xi\rangle$ is the proof of $\mathbf{auth}(\chi, \eta, t\sigma)$ obtained by eliminating the connective $\Rightarrow$ from $|\Xi| \Rightarrow \mathbf{auth}(\chi, \eta, t\sigma)$). Also, the fact that the new proof exists is recorded by updating $\Xi$ to $\Xi' = \Xi[(\chi, \eta, t\sigma) \mapsto \gamma]$, and using $\Xi'$ to compile the remaining program $P$. If the proof construction fails, rule **(Comp dynamic)** is used: the compiler generates code both to construct the proof at run time and to inject it into the system interface. Accordingly, $\mathsf{assert}\ (\eta, t)$ is compiled to $\alpha = \mathsf{prove}\ (\eta, t); \mathsf{inject}\ (\eta, t)\ \alpha$. Even in this case, it is safe to assume that a proof of $\mathbf{auth}(\chi, \eta, t\sigma)$ will exist when $P$ executes (else $\alpha = \mathsf{prove}\ (\eta, t)$ will block at run time), so $\Xi$ is updated to $\Xi' = \Xi[(\chi, \eta, t\sigma) \mapsto \alpha]$.

### Formal Guarantees

We close this section by stating two theorems that guarantee correctness of compilation. Proofs of these theorems can be found in the related technical report [10]. We begin by defining a preorder $\leq$ on system states. Roughly, $H \leq H'$ if any formula that holds under $H$ also holds under $H'$.

**Definition 4.1** ($\leq$)**.** *For any $H$ and $H'$, let $H \leq H'$ if for all $\varphi$, $\gamma$, $\mathcal{L}$, and $s$, (1) $H \vDash \varphi$ implies $H' \vDash \varphi$, and (2) $\gamma :: H; \mathcal{L} \vdash s$ implies $\gamma :: H'; \mathcal{L} \vdash s$.*

Next, we assume the following axioms for the various external judgments. Roughly, Axiom (1) states that system states are updated monotonically by shell command executions. Axioms (2), (3), and (4) state that verification of proofs must be closed under substitution, modus ponens, and product. Axiom (5) states that the theorem prover produces only verifiable proofs (*i.e.*, the theorem prover is sound). Axiom (6) states that the theorem prover always produces a proof if some proof exists (*i.e.*, the theorem prover is complete).

### Axioms

(1) if $H, S \overset{n(t_1\sigma,\ldots,t_k\sigma)}{\blacktriangleright} H', S'$ then $H \leq H'$

(2) if $\gamma :: H; \mathcal{L} \vdash s$ then $\gamma\sigma :: H\sigma; \mathcal{L} \vdash s\sigma$

(3) if $\gamma :: H; \mathcal{L} \vdash s$ and $\gamma' :: H; \mathcal{L} \vdash s \Rightarrow s'$ then $(\gamma'\ \gamma) :: H; \mathcal{L} \vdash s'$

(4) if $\gamma_i :: H; \mathcal{L} \vdash s_i$ for each $i \in 1..n$, then $(\prod_{i \in 1..n} \gamma_i) :: H; \mathcal{L} \vdash \bigwedge_{i \in 1...n} s_i$

(5) if $H; \mathcal{L} \vdash s \searrow \gamma$ then $\gamma :: H; \mathcal{L} \vdash s$

(6) if $\gamma :: H; \mathcal{L} \vdash s$ then $H; \mathcal{L} \vdash s \searrow \gamma'$ for some $\gamma'$.

We can now show that compilation preserves the behavior of programs. More precisely, if a program $P$ compiles to a program $P'$ under a system state $H$, and the programs are run from a system state $H'$ such that $H \leq H'$, then $P$ and $P'$ evaluate to the same state.

**Theorem 4.1** (Compilation correctness)**.** *Suppose that Axioms (1–6) hold, and* $(\varnothing, \varnothing, \varnothing) \vdash P \overset{H,\theta,\chi}{\rightsquigarrow} P'$*. Then for all* $A$ *and* $\rho = (H', \_, \_)$ *such that* $H \leq H'$*, we have* $\rho, P \overset{\theta,A}{\longrightarrow}{}^{\star} \rho', Q$ *for some* $Q$ *if and only if* $\rho, P' \overset{\theta,A}{\longrightarrow}{}^{\star} \rho', Q'$ *for some* $Q'$*.* ($\overset{\theta,A}{\longrightarrow}{}^{\star}$ denotes the reflexive-transitive closure of $\overset{\theta,A}{\longrightarrow}$)

Finally, we show that a compiled program can never fail due to an access check, if the policy does not change between compile time and run time. Formally, compilation preserves the behavior of programs even if the compiled programs are run without access checks.

**Definition 4.2** ($\Longrightarrow$)**.** *Let* $\Longrightarrow$ *be the same reduction relation as* $\longrightarrow$ *except that the rule* **(Reduct shell)** *is replaced by the following rule, which differs from the earlier version in that its premises do not mention any proofs.*

$$\frac{\theta = (\Delta, \mathcal{L}) \qquad \Delta(n) = \eta_1, \ldots, \eta_k \qquad \rho = (H, S, \xi) \qquad H, S \overset{n(t_1,\ldots,t_k)}{\blacktriangleright} H', S' \qquad \rho' = (H', S', \xi)}{\rho, \mathsf{shell}\ n(t_1, \ldots, t_k); P \overset{\theta,\chi}{\longrightarrow} \rho', P}$$

**Theorem 4.2** (Access control redundancy)**.** *Suppose that Axioms (1–6) hold, and* $(\varnothing, \varnothing, \varnothing) \vdash P \overset{H,\theta,\chi}{\rightsquigarrow} P'$*. Then for all* $A$ *and* $\rho = (H', \_, \_)$ *such that* $H \leq H'$*, we have* $\rho, P' \overset{\theta,A}{\longrightarrow}{}^{\star} \rho', Q$ *for some* $Q$ *if and only if* $\rho, P' \overset{\theta,A}{\Longrightarrow}{}^{\star} \rho', Q'$ *for some* $Q'$*.*

Before we close this section, let us point out some consequences of our axioms. Axioms (2), (3), (4), (5) represent standard expectations from the proof system and the theorem prover. Axiom (6) is required to prove soundness of the compiler ("if" direction of Theorem 4.1) since, in its absence, there is no guarantee that a statically provable authorization will be successfully proved in the rule **(Reduct assert)** when executing the source program directly. Axiom (1) is needed for a similar purpose; without this axiom, the compiler must throw away assumptions on the system state in the continuation of any shell command. However, the axiom may seem too strong and invalid in practice. Fortunately, weaker versions of this axiom suffice to prove our theorems for specific programs. In particular, the definition of $H \leq H'$ may be qualified to require that $H \vDash \varphi$ imply $H' \vDash \varphi$ for only those $\varphi$ that appear in a program of interest (and their substitution instances).

# 5 Implementation

We have implemented a prototype PCAL compiler and tested it on the proof-carrying file system PCFS [18]. The specific logic currently used in our implementation is BL [16, 18]. The interested reader can find a complete example (involving homework management between instructors and students of various courses) in the appendix. We now discuss some implementation details that are left abstract in Section 4.

**Rewrite rules**

A set of rewrite rules over terms, modeling abstract properties of the concrete implementations of function symbols, can be provided to the compiler to improve its precision. The compiler constructs a normalization function based on these rules, and applies this function eagerly to substitutions. This works well even in cases where it is not possible to interpret function symbols with directed clauses in the policy. (Modeling equations as clauses usually causes proof searches to loop.)

**Quantified proofs**

Statically generated proofs may contain free variables, and as such they are *parametric* over those variables. In the formal semantics, such proofs are bound and carried as values in the language (in inject statements), so they get implicitly instantiated before injection at run time. However in our actual implementation, such proofs are output to temporary files with distinct names (under `/.pf`), and the names are carried in the language; so the free variables in such proofs must be explicitly substituted at run time. This explains why we considered an explicit `-subst` option to the `inject` command in Section 2.

# 6 Conclusion

PCAL combines static checks and dynamic theorem proving to automate correct and efficient use of a PCA-based interface. PCAL's compiler is modular: it is parametric over both the shell commands (system interface) and the logic it supports. Although this makes the compiler flexible, the interaction between the core language, shell commands, and the logic is subtle and requires careful design. The compiler is made practical through a combination of simple user annotations, static constraint tracking, dynamically checked assertions, and run time support from a command line theorem prover. We prove formally that these ideas work well together. It is our belief that PCAL's design is novel, and that it will be a useful stepping stone for languages that support rule-based access control interfaces in future.

There are several interesting avenues for future work. An obvious one is to run realistic examples on PCAL, to determine what other features are needed in practice. Another possible direction is a code execution architecture where a trusted PCAL compiler is used to generate certified scripts that are run with minimal access control checks. Finally, it will be interesting to apply ideas from PCAL, particularly the use of an automatic theorem prover, in the context of language-based security for access control interfaces (*e.g.*, [4, 20]).

# References

[1] Martín Abadi. Access control in a core calculus of dependency. *Electronic Notes in Theoretical Computer Science*, 172:5–31, 2007. *Computation, Meaning, and Logic: Articles dedicated to Gordon Plotkin.*

[2] Martín Abadi, Michael Burrows, Butler Lampson, and Gordon Plotkin. A calculus for access control in distributed systems. *ACM Transactions on Programming Languages and Systems*, 15(4):706–734, 1993.

[3] Andrew W. Appel and Edward W. Felten. Proof-carrying authentication. In *ACM Conference on Computer and Communications Security (CCS '09)*, pages 52–62. ACM, 1999.

[4] Kumar Avijit, Anupam Datta, and Robert Harper. $\text{PCML}_5$: A language for ensuring compliance with access control policies, 2009. Draft, personal communication.

[5] Lujo Bauer. *Access Control for the Web via Proof-Carrying Authorization*. PhD thesis, Princeton University, 2003.

[6] Lujo Bauer, Scott Garriss, Jonathan M. McCune, Michael K. Reiter, Jason Rouse, and Peter Rutenbar. Device-enabled authorization in the Grey system. In *Information Security Conference (ISC '05)*, LNCS, pages 431–445, 2005.

[7] Moritz Y. Becker, Cédric Fournet, and Andrew D. Gordon. Design and semantics of a decentralized authorization language. In *IEEE Computer Security Foundations Symposium (CSF '07)*, pages 3–15. IEEE, 2007.

[8] Jesper Bengtson, Karthikeyan Bhargavan, Cédric Fournet, Andrew Gordon, and Sergio Maffeis. Refinement types for secure implementations. In *IEEE Computer Security Foundations Symposium (CSF '08)*, pages 17–32. IEEE, 2008.

[9] Avik Chaudhuri and Martín Abadi. Secrecy by typing and file-access control. In *IEEE Computer Security Foundations Workshop (CSFW'06)*, pages 112–123. IEEE, 2006.

[10] Avik Chaudhuri and Deepak Garg. PCAL: Language support for proof-carrying authorization systems. Technical Report CMU-CS-09-141, Carnegie Mellon University, 2009.

[11] Avik Chaudhuri, Prasad Naldurg, and Sriram Rajamani. A type system for data-flow integrity on Windows Vista. In *ACM SIGPLAN Workshop on Programming Languages and Analysis for Security (PLAS'08)*, pages 89–100. ACM, 2008.

[12] John DeTreville. Binder, a logic-based security language. In *IEEE Symposium on Security and Privacy (S&P'02)*, pages 105–113. IEEE, 2002.

[13] Cormac Flanagan. Hybrid type checking. In *ACM Symposium on Principles of Programming Languages (POPL'06)*, pages 245–256. ACM, 2006.

[14] Cédric Fournet, Andrew Gordon, and Sergio Maffeis. A type discipline for authorization in distributed systems. In *IEEE Computer Security Foundations Symposium (CSF '07)*, pages 31–48. IEEE, 2007.

[15] Deepak Garg. Principal-centric reasoning in constructive authorization logic. Technical Report CMU-CS-09-120, Carnegie Mellon University, 2009.

[16] Deepak Garg. Proof search in an authorization logic. Technical Report CMU-CS-09-121, Carnegie Mellon University, 2009.

[17] Deepak Garg and Frank Pfenning. Non-interference in constructive authorization logic. In *IEEE Computer Security Foundations Workshop (CSFW '06)*, pages 283–293. IEEE, 2006.

[18] Deepak Garg and Frank Pfenning. A proof-carrying file system. Technical Report CMU-CS-09-123, Carnegie Mellon University, 2009.

[19] Yuri Gurevich and Itay Neeman. DKAL: Distributed-knowledge authorization language. In *21st IEEE Symposium on Computer Security Foundations (CSF-21)*, 2008.

[20] Limin Jia, Jeffrey A. Vaughan, Karl Mazurak, Jianzhou Zhao, Luke Zarko, Joseph Schorr, and Steve Zdancewic. Aura: A programming language for authorization and audit. In *ACM International Conference on Functional Programming (ICFP '08)*. ACM, 2008.

[21] Butler Lampson, Martín Abadi, Michael Burrows, and Edward Wobber. Authentication in distributed systems: Theory and practice. *ACM Transactions on Computer Systems*, 10(4):265–310, November 1992.

[22] Chris Lesniewski-Laas, Bryan Ford, Jacob Strauss, Robert Morris, and M. Frans Kaashoek. Alpaca: Extensible authorization for distributed services. In *ACM Conference on Computer and Communications Security (CCS '07)*. ACM, 2007.

[23] Andrew Pimlott and Oleg Kiselyov. Soutei, a logic-based trust-management system. In *Eighth International Symposium on Functional and Logic Programming (FLOPS 2006)*, pages 130–145, 2006.

[24] Jeffrey A. Vaughan, Limin Jia, Karl Mazurak, and Steve Zdancewic. Evidence-based audit. In *IEEE Symposium on Computer Security Foundations (CSF '08)*. IEEE, 2008.

# A Proofs

## A.1 Proof of Theorem 4.1

In the following proof, we use a non-deterministic version of our compilation relation, with the following changes.

1. (**Comp static**) can guess any proof that works, not necessarily a proof returned by the theorem prover.

$$\frac{\begin{array}{c}\Gamma = (\sigma, \Phi, \Xi) \qquad \theta = (\_, \mathcal{L}) \\ \gamma' :: H, \Phi; \mathcal{L} \vdash |\Xi| \Rightarrow \mathbf{auth}(\chi, \eta, t\sigma) \qquad \gamma = \gamma'\ \langle \Xi \rangle = \overline{\gamma}\sigma \\ \Xi' = \Xi[(\chi, \eta, t\sigma) \mapsto \gamma] \qquad \Gamma' = (\sigma, \Phi, \Xi') \qquad \Gamma' \vdash P \overset{H,\theta,\chi}{\rightsquigarrow} P'\end{array}}{\Gamma \vdash \mathsf{assert}\ (\eta, t); P \overset{H,\theta,\chi}{\rightsquigarrow} \mathsf{inject}\ (\eta, t)\ \overline{\gamma}; P'}$$

2. (**Comp dynamic**) can be applied whenever (**Comp static**) can be applied.

$$\frac{\begin{array}{c}\Gamma = (\sigma, \Phi, \Xi) \qquad \theta = (\_, \mathcal{L}) \qquad \alpha \text{ fresh in } \Gamma, P \\ \Xi' = \Xi[(\chi, \eta, t\sigma) \mapsto \alpha] \qquad \Gamma' = (\sigma, \Phi, \Xi') \qquad \Gamma' \vdash P \overset{H,\theta,\chi}{\rightsquigarrow} P'\end{array}}{\Gamma \vdash \mathsf{assert}\ (\eta, t); P \overset{H,\theta,\chi}{\rightsquigarrow} \alpha = \mathsf{prove}\ (\eta, t); \mathsf{inject}\ (\eta, t)\ \alpha; P'}$$

Note that these changes allow some more programs to be compiled, but no less; thus, they do not affect the soundness of our results.

We begin with a few basic lemmas. We assume that if $(\sigma, \Phi, \Xi) \vdash P \overset{H,\theta,\chi}{\rightsquigarrow} P'$ then $(\mathsf{fv}(\Phi) \cup \mathsf{fv}(\Xi)) \cap \mathsf{dom}(\sigma) = \varnothing$; note that this invariant is preserved by our typing rules.

**Lemma A.1.** *Suppose that* $(\sigma, \Phi, \Xi) \vdash P \overset{H,\theta,\chi}{\rightsquigarrow} P'$ *and* $x \notin \mathsf{dom}(\sigma)$.
*Then* $(\sigma[x \mapsto t\sigma], \Phi\{t\sigma/x\}, \Xi\{t\sigma/x\}) \vdash P \overset{H,\theta,\chi}{\rightsquigarrow} P'$.

*Proof.* By induction on the derivation of the compilation judgment for $P$. The only interesting case is (**Comp static**), where we use Axiom (2).

**Case** $P = \mathsf{assert}\ (\eta, t); \widehat{Q}$ and $P' = \mathsf{inject}\ (\eta, t)\ \gamma; \widehat{Q'}$
such that $\theta = (\_, \mathcal{L})$,
$\gamma' :: H, \Phi; \mathcal{L} \vdash |\Xi| \Rightarrow \mathbf{auth}(\chi, \eta, t\sigma)$,
$\gamma = \gamma'\ \langle \Xi \rangle$,
$\widehat{\Xi} = \Xi[(\chi, \eta, t\sigma) \mapsto \gamma]$,
and $(\sigma, \Phi, \widehat{\Xi}) \vdash \widehat{Q} \overset{H,\theta,\chi}{\rightsquigarrow} \widehat{Q'}$.
Let $\sigma' = \{t'\sigma/x\}$.
We require $(\sigma[x \mapsto t'\sigma], \Phi\sigma', \Xi\sigma') \vdash P \overset{H,\theta,\chi}{\rightsquigarrow} P'$.
By Axiom (2), $\gamma'\sigma' :: H, \Phi\sigma'; \mathcal{L} \vdash |\Xi\sigma'| \Rightarrow \mathbf{auth}(\chi, \eta, t\sigma\sigma')$.
Also, by assumption, $(\sigma[x \mapsto t'\sigma], \Phi\sigma', \widehat{\Xi}\sigma') \vdash \widehat{Q} \overset{H,\theta,\chi}{\rightsquigarrow} \widehat{Q'}$.
The result follows.

□

**Lemma A.2.** *Suppose that* $(\sigma[x \mapsto t\sigma], \Phi, \Xi) \vdash P \overset{H,\theta,\chi}{\rightsquigarrow} P'$.
*Then* $(\sigma, \Phi, \Xi) \vdash P\{t/x\} \overset{H,\theta,\chi}{\rightsquigarrow} P'\{t/x\}$.

*Proof.* By induction on the derivation of the compilation judgment for $P$. □

**Lemma A.3.** *Suppose that* $(\sigma, \Phi, \Xi) \vdash P \overset{H,\theta,\chi}{\rightsquigarrow} P'$, $\widetilde{x} = \mathcal{W}(P)$, *and* $(\sigma\backslash\widetilde{x}, \Phi, \Xi) \vdash Q \overset{H,\theta,\chi}{\rightsquigarrow} Q'$. *Then* $(\sigma, \Phi, \Xi) \vdash P; Q \overset{H,\theta,\chi}{\rightsquigarrow} P'; Q'$.

*Proof.* By induction on the derivation of the compilation judgment for $P$. The only interesting cases are (**Comp assign**), where we use Lemma A.1, and (**Comp for**) and (**Comp test**), which are similar but do not require any additional lemma. Let $\Gamma = (\sigma, \Phi, \Xi)$.

**Case** $P = \mathsf{for}\ x\ \mathsf{in}\ t\ \{\widehat{P}\}; \widehat{Q}$

Then $P' = \mathsf{for}\ x\ \mathsf{in}\ t\ \{\widehat{P'}\}; \widehat{Q'}$ such that
$x$ is fresh in $\Gamma$,
$\widehat{\Phi} = \Phi, \mathtt{member}(x, t\sigma)$,
$\widetilde{z} = \mathcal{W}(\widehat{P})$,
$(\sigma\backslash\widetilde{z}, \widehat{\Phi}, \Xi) \vdash \widehat{P} \overset{H,\theta,\chi}{\rightsquigarrow} \widehat{P'}$,
and $(\sigma\backslash\widetilde{z}, \Phi, \Xi) \vdash \widehat{Q} \overset{H,\theta,\chi}{\rightsquigarrow} \widehat{Q'}$.
By assumption, $\widetilde{x} = \widetilde{z} \cup \mathcal{W}(\widehat{Q})$
and $(\sigma\backslash\widetilde{x}, \Phi, \Xi) \vdash Q \overset{H,\theta,\chi}{\rightsquigarrow} Q'$.
We need $(\sigma\backslash\widetilde{z}, \Phi, \Xi) \vdash \widehat{Q}; Q \overset{H,\theta,\chi}{\rightsquigarrow} \widehat{Q'}; Q'$.
The result follows by the inductive hypothesis.

**Case** $P = \mathsf{test}\ \varphi\ \{\widehat{P}\}; \widehat{Q}$

Then $P' = \mathsf{test}\ \varphi\ \{\widehat{P'}\}; \widehat{Q'}$ such that
$\widetilde{z} = \mathcal{W}(\widehat{P})$,
$\widehat{\Phi} = \Phi, \varphi\sigma$,
$(\sigma, \widehat{\Phi}, \Xi) \vdash \widehat{P} \overset{H,\theta,\chi}{\rightsquigarrow} \widehat{P'}$,
and $(\sigma\backslash\widetilde{z}, \Phi, \Xi) \vdash \widehat{Q} \overset{H,\theta,\chi}{\rightsquigarrow} \widehat{Q'}$.
By assumption, $\widetilde{z} = \widetilde{x} \cup \mathcal{W}(\widehat{Q})$
and $(\sigma\backslash\widetilde{x}, \Phi, \Xi) \vdash Q \overset{H,\theta,\chi}{\rightsquigarrow} Q'$.
We need $(\sigma\backslash\widetilde{z}, \Phi, \Xi) \vdash \widehat{Q}; Q \overset{H,\theta,\chi}{\rightsquigarrow} \widehat{Q'}; Q'$.
The result follows by the inductive hypothesis.

**Case** $P = (x = t; \widehat{Q})$

Then $P' = (x = t; \widehat{Q'})$ such that
$(\sigma[x \mapsto t\sigma], \Phi, \Xi) \vdash \widehat{Q} \overset{H,\theta,\chi}{\rightsquigarrow} \widehat{Q'}$.
By assumption, $\widetilde{x} = \{x\} \cup \mathcal{W}(\widehat{Q})$
and $(\sigma\backslash\widetilde{x}, \Phi, \Xi) \vdash Q \overset{H,\theta,\chi}{\rightsquigarrow} Q'$.
We need $(\sigma[x \mapsto t\sigma], \Phi, \Xi) \vdash \widehat{Q}; Q \overset{H,\theta,\chi}{\rightsquigarrow} \widehat{Q'}; Q'$.
Let

- $x \in \mathcal{W}(\widehat{Q})$.
  The result follows by the inductive hypothesis.

- $x \notin \mathcal{W}(\widehat{Q})$.
  Then $\sigma\backslash W(\widehat{Q}) = (\sigma\backslash\widetilde{x})[x \mapsto t\sigma]$.
  The result follows by Lemma A.1 and the inductive hypothesis.

□

Building on these basic lemmas, the proof of Theorem 4.1 relies on the following main lemma. Here, we write $\overline{\sigma} <_\mu \sigma$ when $\overline{\sigma}\mu = \sigma$ and $\mu$ only substitutes proofs. Note that since terms $t$ and propositions $\varphi$ cannot contain proof variables, we always have $t\mu = t$ and $\varphi\mu = \varphi$.

**Lemma A.4.** *Suppose that Axioms (1–6) hold. Let $\sigma$ be any ground substitution, and $\overline{\sigma}$, $\mu$ be such that $\overline{\sigma} <_\mu \sigma$. Let $\theta = \_, \mathcal{L}$. Let $\overline{H}$, $\Phi$, $\Xi$, $H$, and $\xi$ be such that $H \vDash \overline{H}, \Phi$ and $\forall(\chi, \eta, t) \in \mathsf{dom}(\Xi)$, we have $H; \mathcal{L} \vdash \mathbf{auth}(\chi, \eta, t) \searrow \xi(\chi, \eta, t)$ and $\Xi(\chi, \eta, t)\mu :: H; \mathcal{L} \vdash \mathbf{auth}(\chi, \eta, t)$.*

*Suppose that $(\overline{\sigma}, \Phi, \Xi) \vdash P \overset{\overline{H},\theta,\chi}{\rightsquigarrow} P'$.*

- *If $H, S, \xi, P\sigma \xrightarrow{\theta,\chi} H', S', \xi', Q\sigma'$ for some $Q$ and $\sigma'$ then*
  *$H, S, \Xi\mu, P'\sigma \xrightarrow{\theta,\chi} H', S', \Xi'\mu', Q'\sigma'$ for some $Q'$, $\mu'$, $\Phi'$, and $\Xi'$ such that*
  *$\overline{\sigma} <_{\mu'} \sigma'$, $(\overline{\sigma}, \Phi', \Xi') \vdash Q \overset{\overline{H},\theta,\chi}{\rightsquigarrow} Q'$, $H' \vDash \overline{H}, \Phi'$, and $\forall(\chi, \eta, t) \in \mathsf{dom}(\Xi')$: $H'; \mathcal{L} \vdash \mathbf{auth}(\chi, \eta, t) \searrow \xi'(\chi, \eta, t)$ and $\Xi'(\chi, \eta, t)\mu' :: H'; \mathcal{L} \vdash \mathbf{auth}(\chi, \eta, t)$.*

- *If $H, S, \Xi\mu, P'\sigma \xrightarrow{\theta,\chi} H', S', \xi'', Q'\sigma'$ for some $\xi''$, $Q'$, and $\sigma'$ then $\xi'' = \Xi'\mu'$*
  *and $H, S, \xi, P\sigma \xrightarrow{\theta,\chi}{}^{?} H', S', \xi', Q\sigma'$ for some $Q$, $\mu'$, $\Phi'$, and $\Xi'$ such that*
  *$\overline{\sigma} <_{\mu'} \sigma'$, $(\overline{\sigma}, \Phi', \Xi') \vdash Q \overset{\overline{H},\theta,\chi}{\rightsquigarrow} Q'$, $H' \vDash \overline{H}, \Phi'$, and $\forall(\chi, \eta, t) \in \mathsf{dom}(\Xi')$: $H'; \mathcal{L} \vdash \mathbf{auth}(\chi, \eta, t) \searrow \xi'(\chi, \eta, t)$ and $\Xi'(\chi, \eta, t)\mu' :: H'; \mathcal{L} \vdash \mathbf{auth}(\chi, \eta, t)$.*
  *(Note: $\xrightarrow{\theta,\chi}{}^{?}$ denotes zero or one steps of $\xrightarrow{\theta,\chi}$)*

*Proof.* By induction on the derivation of the compilation judgment for $P$. Let $\Gamma = (\overline{\sigma}, \Phi, \Xi)$.

**Case** $P = \mathsf{for}\ x\ \mathsf{in}\ t\ \{\widehat{P}\}; \widehat{Q}$
Then $P' = \mathsf{for}\ x\ \mathsf{in}\ t\ \{\widehat{P'}\}; \widehat{Q'}$ such that
$x$ is fresh in $\Gamma$,
$\widehat{\Phi} = \Phi, \mathtt{member}(x, t\overline{\sigma})$,
$\widetilde{x} = \mathcal{W}(\widehat{P})$,
$(\overline{\sigma}\backslash\widetilde{x}, \widehat{\Phi}, \Xi) \vdash \widehat{P} \overset{\overline{H},\theta,\chi}{\rightsquigarrow} \widehat{P'}$,
and $(\overline{\sigma}\backslash\widetilde{x}, \Phi, \Xi) \vdash \widehat{Q} \overset{\overline{H},\theta,\chi}{\rightsquigarrow} \widehat{Q'}$.
Furthermore, let

- $H' = H$,
  $S' = S$,
  $\xi' = \xi$,

$\sigma' = \sigma$,
and $Q = \widehat{P}\sigma_1; \ldots; \widehat{P}\sigma_k; \widehat{Q}$ such that
$\texttt{members}(H, t\sigma) = t_1, \ldots, t_k$
and $\sigma_1 = \{t_1/x\}, \ldots, \sigma_k = \{t_k/x\}$.
Then $Q' = \widehat{P'}\sigma_1; \ldots; \widehat{P'}\sigma_k; \widehat{Q'}$.
We require $(\overline{\sigma}, \Phi', \Xi') \vdash Q \overset{\overline{H},\theta,\chi}{\rightsquigarrow} Q'$ for some $\Phi', \Xi'$.
Let $\Phi' = \Phi, \texttt{member}(t_1, t\overline{\sigma}), \ldots, \texttt{member}(t_k, t\overline{\sigma})$
and $\Xi' = \Xi$.
Using the freshness assumption on $x$:
By Lemmas A.1 and A.2 and weakening, $(\overline{\sigma}\backslash\widetilde{x}, \Phi', \Xi') \vdash \widehat{P}\sigma_i \overset{\overline{H},\theta,\chi}{\rightsquigarrow} \widehat{P'}\sigma_i$.
Furthermore, by weakening, $(\overline{\sigma}\backslash\widetilde{x}, \Phi', \Xi') \vdash \widehat{Q} \overset{\overline{H},\theta,\chi}{\rightsquigarrow} \widehat{Q'}$.
By Lemma A.3, $(\overline{\sigma}\backslash\widetilde{x}, \Phi', \Xi') \vdash \widehat{P}\sigma_1; \ldots; \widehat{P}\sigma_k; \widehat{Q} \overset{\overline{H},\theta,\chi}{\rightsquigarrow} \widehat{P'}\sigma_1; \ldots; \widehat{P'}\sigma_k; \widehat{Q'}$.
By construction, $\mathsf{dom}(\overline{\sigma'}) \cap (\mathsf{fv}(\Phi') \cup \mathsf{fv}(\Xi')) = \varnothing$.
The required result follows by Lemma A.1.
Finally, we have
$\overline{\sigma} <_{\mu'} \sigma'$ where $\mu' = \mu$,
$H' \vDash \overline{H}, \Phi'$ (by assumption on `members` and `member`, since $\overline{\sigma}\mu' = \sigma$),
and $\forall(\chi, \eta, t) \in \Xi' :$
$\Xi'(\chi, \eta, t)\mu' :: H'; \mathcal{L} \vdash \mathbf{auth}(\chi, \eta, t)$ and $H'; \mathcal{L} \vdash \mathbf{auth}(\chi, \eta, t) \searrow \xi'(\chi, \eta, t)$.

- The converse case is similar.

**Case** $P = \mathsf{test}\ \varphi\ \{\widehat{P}\}; \widehat{Q}$
Then $P' = \mathsf{test}\ \varphi\ \{\widehat{P'}\}; \widehat{Q'}$ such that
$\widetilde{x} = \mathcal{W}(\widehat{P})$,
$\widehat{\Phi} = \Phi, \varphi\overline{\sigma}$,
$(\overline{\sigma}, \widehat{\Phi}, \Xi) \vdash \widehat{P} \overset{\overline{H},\theta,\chi}{\rightsquigarrow} \widehat{P'}$,
and $(\overline{\sigma}\backslash\widetilde{x}, \Phi, \Xi) \vdash \widehat{Q} \overset{\overline{H},\theta,\chi}{\rightsquigarrow} \widehat{Q'}$.
Furthermore, let

- $H' = H$,
  $S' = S$,
  $\xi' = \xi$,
  $\sigma' = \sigma$,
  and $Q = \widehat{P}; \widehat{Q}$ such that
  $H \vDash \varphi\sigma$.
  Then $Q' = \widehat{P'}; \widehat{Q'}$.
  We require $(\overline{\sigma}, \Phi', \Xi') \vdash Q \overset{\overline{H},\theta,\chi}{\rightsquigarrow} Q'$ for some $\Phi', \Xi'$.
  Let $\Phi' = \widehat{\Phi}$
  and $\Xi' = \Xi$.

By Lemma A.3 and weakening, we have the required result.
Finally, we have
$\overline{\sigma} <_{\mu'} \sigma'$ where $\mu' = \mu$,
$H' \vDash \overline{H}, \Phi'$ (by assumption above),
and $\forall(\chi, \eta, t) \in \Xi' :$
$\Xi'(\chi, \eta, t)\mu' :: H'; \mathcal{L} \vdash \mathbf{auth}(\chi, \eta, t)$ and $H'; \mathcal{L} \vdash \mathbf{auth}(\chi, \eta, t) \searrow \xi'(\chi, \eta, t)$.

- $H' = H$,
  $S' = S$,
  $\xi' = \xi$,
  $\sigma' = \sigma$,
  and $Q = \widehat{Q}$ such that
  $H \nvDash \varphi\sigma$.
  Then $Q' = \widehat{Q'}$.
  We require $(\overline{\sigma}, \Phi', \Xi') \vdash Q \overset{\overline{H},\theta,\chi}{\rightsquigarrow} Q'$ for some $\Phi', \Xi'$.
  Let $\Phi' = \Phi$,
  and $\Xi' = \Xi$.
  By construction, $\mathsf{dom}(\overline{\sigma}') \cap (\mathsf{fv}(\Phi') \cup \mathsf{fv}(\Xi')) = \varnothing$.
  So the required result follows by Lemma A.1.
  Finally, we have
  $\overline{\sigma} <_{\mu'} \sigma'$ where $\mu' = \mu$,
  $H' \vDash \overline{H}, \Phi'$,
  and $\forall(\chi, \eta, t) \in \Xi' :$
  $\Xi'(\chi, \eta, t)\mu' :: H'; \mathcal{L} \vdash \mathbf{auth}(\chi, \eta, t)$ and $H'; \mathcal{L} \vdash \mathbf{auth}(\chi, \eta, t) \searrow \xi'(\chi, \eta, t)$.
- The converse case is similar.

**Case** $P = (x = t; \widehat{Q})$
Then $P' = (x = t; \widehat{Q'})$ such that
$(\overline{\sigma}[x \mapsto t\overline{\sigma}], \Phi, \Xi) \vdash \widehat{Q} \overset{\overline{H},\theta,\chi}{\rightsquigarrow} \widehat{Q'}$.
Furthermore, let

- $H' = H$,
  $S' = S$,
  $\xi' = \xi$,
  $\sigma' = \sigma$,
  and $Q = \widehat{Q}\{t\overline{\sigma}/x\}$.
  Then $Q' = \widehat{Q'}\{t\overline{\sigma}/x\}$.
  We require $(\overline{\sigma}, \Phi', \Xi') \vdash Q \overset{\overline{H},\theta,\chi}{\rightsquigarrow} Q'$ for some $\Phi', \Xi'$.
  Let $\Phi' = \Phi$,
  and $\Xi' = \Xi$.
  By Lemma A.2 we have the required result.

Finally, we have
$\overline{\sigma} <_{\mu'} \sigma'$ where $\mu' = \mu$,
$H' \vDash \overline{H}, \Phi'$,
and $\forall (\chi, \eta, t) \in \Xi' :$
$\Xi'(\chi, \eta, t)\mu' :: H'; \mathcal{L} \vdash \mathbf{auth}(\chi, \eta, t)$ and $H'; \mathcal{L} \vdash \mathbf{auth}(\chi, \eta, t) \searrow \xi'(\chi, \eta, t)$.

- The converse case is similar.

**Case** $P = \mathsf{shell}\ n(t_1, \ldots, t_k); \widehat{Q}$
Then $P' = \mathsf{shell}\ n(t_1, \ldots, t_k); \widehat{Q'}$ such that
$\theta = (\Delta, \mathcal{L})$,
$\Delta(n) = \eta_1, \ldots, \eta_k$,
$(\chi, \eta_i, t_i\overline{\sigma}) \in \mathsf{dom}(\Xi)$ for each $i$,
and $(\overline{\sigma}, \Phi, \Xi) \vdash \widehat{Q} \overset{\overline{H}, \theta, \chi}{\rightsquigarrow} \widehat{Q'}$.
Furthermore, let

- $\xi' = \xi$,
  $\sigma' = \sigma$,
  and $Q = \widehat{Q}$ such that
  $H, S \overset{n(t_1\sigma, \ldots, t_k\sigma)}{\blacktriangleright} H', S'$,
  $\xi(\chi, \eta_i, t_i\sigma) = \gamma_i$ for each $i$,
  and $\gamma_i :: H; \mathcal{L} \vdash \mathbf{auth}(\chi, \eta_i, t_i\sigma)$ for each $i$.
  (Note that we have $H; \mathcal{L} \vdash \mathbf{auth}(\chi, \eta_i, t_i\sigma) \searrow \xi(\chi, \eta_i, t_i\sigma)$ for each $i$.
  So by Axiom (5) we do not need the proof-checking above.)
  Let $\Xi(\chi, \eta_i, t_i\sigma)\mu = \overline{\gamma_i}$ for each $i$.
  By assumption, $\overline{\gamma_i} :: H; \mathcal{L} \vdash \mathbf{auth}(\chi, \eta_i, t_i\sigma)$ for each $i$.
  Then $Q' = \widehat{Q'}$.
  We require $(\overline{\sigma}, \Phi', \Xi') \vdash Q \overset{\overline{H}, \theta, \chi}{\rightsquigarrow} Q'$ for some $\Phi', \Xi'$.
  Let $\Phi' = \Phi$,
  and $\Xi' = \Xi$.
  Then we have the required result.
  Finally, we have
  $\overline{\sigma} <_{\mu'} \sigma'$ where $\mu' = \mu$,
  $H' \vDash \overline{H}, \Phi'$ (by Axiom (1) and assumption on $\leq$ and $\vDash$),
  and $\forall (\chi, \eta, t) \in \Xi' :$
  $\Xi'(\chi, \eta, t)\mu' :: H'; \mathcal{L} \vdash \mathbf{auth}(\chi, \eta, t)$ and $H'; \mathcal{L} \vdash \mathbf{auth}(\chi, \eta, t) \searrow \xi'(\chi, \eta, t)$.
- The converse case is similar.

**Case** $P = \mathsf{assert}\ (\eta, t); \widehat{Q}$ and $P' = (\alpha = \mathsf{prove}\ (\eta, t); \mathsf{inject}\ (\eta, t)\ \alpha; \widehat{Q'})$
such that $\theta = (\_, \mathcal{L})$,

$\alpha$ is fresh,
$\widehat{\Xi} = \Xi[(\chi, \eta, t\overline{\sigma}) \mapsto \alpha]$,
$(\overline{\sigma}, \Phi, \widehat{\Xi}) \vdash \widehat{Q} \overset{H,\theta,\chi}{\rightsquigarrow} \widehat{Q'}$.
Furthermore, let

- $H' = H$,
  $S' = S$,
  $\xi' = \xi[(\chi, \eta, t\sigma) \mapsto \gamma]$,
  $\sigma' = \sigma[\alpha \mapsto \gamma]$,
  and $Q = \widehat{Q}$ such that
  $H; \mathcal{L} \vdash \mathbf{auth}(\chi, \eta, t\sigma) \searrow \gamma$.
  Then $Q' = \widehat{Q'}$.

  We require $(\overline{\sigma}, \Phi', \Xi') \vdash Q \overset{\overline{H},\theta,\chi}{\rightsquigarrow} Q'$ for some $\Phi', \Xi'$.
  Let $\Phi' = \Phi$,
  and $\Xi' = \widehat{\Xi}$.
  Then we have the required result.
  Finally, we have
  $\overline{\sigma} <_{\mu'} \sigma'$ where $\mu' = \mu[\alpha \mapsto \gamma]$,
  $H' \vDash \overline{H}, \Phi'$,
  and $\forall (\chi, \eta, t) \in \Xi' :$
  $\Xi'(\chi, \eta, t)\mu' :: H'; \mathcal{L} \vdash \mathbf{auth}(\chi, \eta, t)$ and $H'; \mathcal{L} \vdash \mathbf{auth}(\chi, \eta, t) \searrow \xi'(\chi, \eta, t)$
  (since in particular, $H'; \mathcal{L} \vdash \mathbf{auth}(\chi, \eta, t\sigma) \searrow \xi'(\chi, \eta, t\sigma)$
  and since $\Xi'(\chi, \eta, t\overline{\sigma})\mu' = \alpha\mu' = \gamma = \xi'(\chi, \eta, t\sigma)$,
  so, by Axiom (5), $\Xi'(\chi, \eta, t\sigma)\mu' :: H'; \mathcal{L} \vdash \mathbf{auth}(\chi, \eta, t)$).
- $H' = H$,
  $S' = S$,
  $\xi'' = \xi$,
  $\sigma' = \sigma$,
  and $Q' = \mathsf{inject}\ (\eta, t)\ \gamma; \widehat{Q}$ such that
  $H; \mathcal{L} \vdash \mathbf{auth}(\chi, \eta, t\sigma) \searrow \gamma$.
  Then $Q = P$.

  We require $(\overline{\sigma}, \Phi', \Xi') \vdash Q \overset{\overline{H},\theta,\chi}{\rightsquigarrow} Q'$ for some $\Phi', \Xi'$.
  Let $\Phi' = \Phi$,
  and $\Xi' = \Xi$.
  By assumption, we already have $H; \mathcal{L} \vdash \mathbf{auth}(\chi, \eta, t\sigma) \searrow \gamma$.

  Now we require $(\overline{\sigma}, \Phi, \Xi[(\chi, \eta, t\sigma) \mapsto \gamma]) \vdash \widehat{Q} \overset{\overline{H},\theta,\chi}{\rightsquigarrow} \widehat{Q'}$.
  Since $\alpha \notin \mathsf{dom}(\overline{\sigma})$, the result follows by Lemma A.1.
  Finally, we have
  $\overline{\sigma} <_{\mu'} \sigma'$ where $\mu' = \mu$,
  $H' \vDash \overline{H}, \Phi'$,
  and $\forall (\chi, \eta, t) \in \Xi' :$

$\Xi'(\chi,\eta,t)\mu' :: H'; \mathcal{L} \vdash \mathbf{auth}(\chi,\eta,t)$ and $H'; \mathcal{L} \vdash \mathbf{auth}(\chi,\eta,t) \searrow \xi'(\chi,\eta,t)$.

**Case** $P = \mathsf{assert}\ (\eta,t); \widehat{Q}$ and $P' = \mathsf{inject}\ (\eta,t)\ \overline{\gamma}; \widehat{Q'}$
such that $\theta = (\_, \mathcal{L})$,
$\overline{H}, \Phi; \mathcal{L} \vdash |\Xi| \Rightarrow \mathbf{auth}(\chi,\eta,t\overline{\sigma}) \searrow \gamma'$,
$\overline{\gamma} = \gamma'\ \langle\Xi\rangle$,
$\widehat{\Xi} = \Xi[(\chi,\eta,t\overline{\sigma}) \mapsto \overline{\gamma}]$,
and $(\overline{\sigma}, \Phi, \widehat{\Xi}) \vdash \widehat{Q} \overset{\overline{H},\theta,\chi}{\rightsquigarrow} \widehat{Q'}$.
Furthermore, let

- $H' = H$,
  $S' = S$,
  $\xi' = \xi[(\chi,\eta,t\sigma) \mapsto \gamma]$,
  $\sigma' = \sigma$,
  and $Q = \widehat{Q}$ such that
  $H; \mathcal{L} \vdash \mathbf{auth}(\chi,\eta,t\sigma) \searrow \gamma$.
  Then $Q' = \widehat{Q'}$
  and $\Xi' = \widehat{\Xi}$.
  We require $(\overline{\sigma}, \Phi', \Xi') \vdash Q \overset{\overline{H},\theta,\chi}{\rightsquigarrow} Q'$ for some $\Phi', \Xi'$.
  Let $\Phi' = \Phi$.
  Then we have the required result.
  Finally, we have
  $\overline{\sigma} <_{\mu'} \sigma'$ where $\mu' = \mu$,
  $H' \vDash \overline{H}, \Phi'$,
  and $\forall(\chi,\eta,t) \in \Xi'$ :
  $\Xi'(\chi,\eta,t)\mu' :: H'; \mathcal{L} \vdash \mathbf{auth}(\chi,\eta,t)$ and $H'; \mathcal{L} \vdash \mathbf{auth}(\chi,\eta,t) \searrow \xi'(\chi,\eta,t)$
  (since in particular, $H'; \mathcal{L} \vdash \mathbf{auth}(\chi,\eta,t\sigma) \searrow \xi'(\chi,\eta,t\sigma)$, and
  since by Axiom (5), $\gamma' :: H; \mathcal{L} \vdash |\Xi| \Rightarrow \mathbf{auth}(\chi,\eta,t\sigma)$,
  and by Axiom (4), $\langle\Xi\rangle\mu :: H; \mathcal{L} \vdash |\Xi|$,
  so by Axiom (3), $\overline{\gamma}\mu' :: H; \mathcal{L} \vdash \mathbf{auth}(\chi,\eta,t\sigma)$).
- $H' = H$,
  $S' = S$,
  $\xi'' = \Xi\mu[(\chi,\eta,t\sigma) \mapsto \overline{\gamma}\mu]$,
  $\sigma' = \sigma$,
  and $Q' = \widehat{Q'}$.
  Let $\Xi' = \widehat{\Xi}$.
  Now, by assumption, we have $H; \mathcal{L} \vdash |\Xi| \Rightarrow \mathbf{auth}(\chi,\eta,t\sigma) \searrow \gamma'$.
  Also, by Axiom (4), we have $\langle\Xi\rangle\mu :: H; \mathcal{L} \vdash |\Xi|$.
  So, by Axiom (5), $\gamma' :: H; \mathcal{L} \vdash |\Xi| \Rightarrow \mathbf{auth}(\chi,\eta,t\sigma)$.
  So, by Axiom (3), $\overline{\gamma}\mu' :: H; \mathcal{L} \vdash \mathbf{auth}(\chi,\eta,t\sigma)$.
  So, by Axiom (6), $H; \mathcal{L} \vdash \mathbf{auth}(\chi,\eta,t\sigma) \searrow \gamma$ for some $\gamma$.

Then $Q = \widehat{Q}$
and $\xi' = \xi[(\chi, \eta, t\sigma) \mapsto \gamma]$.
We require $(\overline{\sigma}, \Phi', \Xi') \vdash Q \overset{\overline{H},\theta,\chi}{\rightsquigarrow} Q'$ for some $\Phi', \Xi'$.
Let $\Phi' = \Phi$.
Then we have the required result.
Finally, we have
$\overline{\sigma} <_{\mu'} \sigma'$ where $\mu' = \mu$,
$H' \vDash \overline{H}, \Phi'$,
and $\forall (\chi, \eta, t) \in \Xi' :$
$\Xi'(\chi, \eta, t)\mu' :: H'; \mathcal{L} \vdash \mathbf{auth}(\chi, \eta, t)$ and $H'; \mathcal{L} \vdash \mathbf{auth}(\chi, \eta, t) \searrow \xi'(\chi, \eta, t)$
(since in particular, $H'; \mathcal{L} \vdash \mathbf{auth}(\chi, \eta, t\sigma) \searrow \xi'(\chi, \eta, t\sigma)$, and
$\overline{\gamma}\mu' :: H; \mathcal{L} \vdash \mathbf{auth}(\chi, \eta, t\sigma)$ as shown above).

□

**Lemma A.5.** *Lemma A.4 implies Theorem 4.1.*

*Proof.* By induction on the length of $\overset{\theta,A}{\longrightarrow}^{\star}$. □

### A.2 Proof of Theorem 4.2

The proof follows by observation of the proof of Lemma A.4. In particular, for the case where $P$ is a shell command, using the relaxed **(Reduct shell)** rule suffices to establish the required invariants.

## B Example: Homework for Courses

Consider the following idealized scenario for homework management of various courses at an university. There is a directory, `"/courses"`, containing the directories of all courses. In each course directory, there is a directory named `"instructor"` and a directory named `"students"`, both containing directories named after all students. Furthermore, the `"instructor"` directory contains a file called `"homework"`, and each directory under `"students"` has a file called `"solution"`.

Figure 4 shows a PCAL program that does the following. It navigates into the `"instructor"` directory, and copies the `"homework"` file into each directory under `"students"` in turn. Then, it navigates into those directories and copies the `"solution"` file of that student into the corresponding directory under `"instructor"`.

Next, we show the policy in effect. The policy is written in the authorization logic BL [15, 16]. In order to represent policies made by different principals, BL includes a modality $A$ **says** $s$ which means that administrator $A$ states, or believes formula $s$ ($s$ usually expresses a policy rule). The **says** modality has been considered in prior work (*e.g.*, [1, 2, 17, 21]), but the inference rules defining its meaning vary. BL's rules are shown below. In addition, any complete axiomatization of first-order intuitionistic logic is also assumed.

```
courses = "/courses";

assert (read, courses);
for course in courses {
  assert (read, course);
  for user in course {
    test suffix (user, "instructor") {
      instructor = user;
      assert (read, instructor);
      for fileinstr in instructor {
        test suffix (fileinstr, "homework") {
          assert (read, fileinstr);
          students = course/"students";
          assert (read, students);
          for studdir in students {
            hwstud = studdir/"homework";
            assert (write, hwstud);
            shell cp (fileinstr, hwstud)
          }
        }
      }
    };

    test suffix (user, "students") {
      assert (read, user);
      for userdir in user {
        studname = base (userdir);
        solninstr = course/"instructor"/studname/"solution";
        solnstud = userdir/"solution";
        assert read solnstud;
        assert write solninstr;
        shell cp (solnstud, solninstr)
      }
    }
  }
}
```

Figure 4: PCAL program for homework example

$$\vdash (A \textbf{ says } (s \Rightarrow t)) \Rightarrow ((A \textbf{ says } s) \Rightarrow (A \textbf{ says } t)) \tag{K}$$

$$\frac{\vdash s}{\vdash A \textbf{ says } s} \tag{N}$$

$$\vdash (A \textbf{ says } s) \Rightarrow (A' \textbf{ says } A \textbf{ says } s) \tag{I}$$

$$\vdash A \textbf{ says } ((A \textbf{ says } s) \Rightarrow s) \tag{C}$$

In our specific policy, we assume that $S$ and $L$ are separate authorities. The formula $\mathbf{auth}(A, \eta, t)$ is defined as $S$ **says** $\mathbf{may}(A, \eta, t)$; in other words, $S$ represents the enforcer of the policy. On the other hand, $L$ is a local authority that may certify some formulas that $S$ relies on, for example, the validity of the `"/courses"` directory and the membership of certain principals in special groups for which certain policy rules may apply.

We focus on a detailed modeling of the relationship between the function symbol / (that concatenates directory paths with file names to to give file paths) and directory membership constraints. This allows the compiler to reason, for example, that if $f$ is in directory $d$ and the suffix of $f$ is $x$ then $f \equiv d/x$. Other rules allow principals in the group `special` to inherit `read` permissions from ancestor directories. Finally, there are rules that are specific to instructors and students, specifying which files in the others' directories they are allowed to read and write.

The policy rules are split into two parts. The first part contains the rules stated by $L$:

$$\forall c.\ (S \textbf{ says } \texttt{member}(c, \texttt{"/courses"})) \Rightarrow \texttt{course}(c)$$

$$\texttt{special}(\texttt{"User"})$$

The next part contains the rules stated by $S$. These include all the policy rules, plus rules that model equivalences between paths constructed using /, `base`, and `suffix`.

$$\forall f.\forall d.\forall x.\ \texttt{member}(f, d) \Rightarrow \texttt{suffix}(f, x) \Rightarrow f \equiv d/x$$
$$\forall f.\forall d.\forall x.\forall p.\ \texttt{member}(f, d) \Rightarrow \texttt{suffix}(f, x) \Rightarrow d \equiv p \Rightarrow f \equiv p/x$$

$$\forall A.\forall f.\forall p.\forall \eta.\ f \equiv p \Rightarrow \mathbf{may}(A, \eta, f) \Rightarrow \mathbf{may}(A, \eta, p)$$

$$\forall f.\ \texttt{suffix}(f, \texttt{base}(x))$$

$$\begin{aligned}\forall A.\forall c.\forall d.\ (L \textbf{ says } \texttt{course}(c)) \Rightarrow \mathbf{may}(A, \texttt{read}, c/\texttt{"instructor"}) \Rightarrow \\ \mathbf{may}(A, \texttt{read}, c/\texttt{"students"}) \\ \wedge\ \texttt{member}(d, c/\texttt{"students"}) \Rightarrow \mathbf{may}(A, \texttt{write}, d/\texttt{"homework"})\end{aligned}$$

$$\begin{aligned}\forall A.\forall c.\forall x.\forall d.\ (L \textbf{ says } \texttt{course}(c)) \Rightarrow \mathbf{may}(A, \texttt{read}, c/\texttt{"students"}/x) \Rightarrow \\ \mathbf{may}(A, \texttt{write}, c/\texttt{"instructor"}/x/\texttt{"solution"}) \\ \wedge\ d \equiv c/\texttt{"students"}/x) \Rightarrow \mathbf{may}(A, \texttt{read}, d/\texttt{"solution"})\end{aligned}$$

$$\begin{aligned}&\forall A.\ \mathbf{may}(A, \texttt{read}, \texttt{"/courses"}) \\ &\forall A.\forall f.\forall d.\ (L \textbf{ says } \texttt{special}(A)) \Rightarrow \texttt{member}(f, d) \Rightarrow \\ &\qquad \mathbf{may}(A, \texttt{read}, d) \Rightarrow \mathbf{may}(A, \texttt{read}, f)\end{aligned}$$

With this policy, the PCAL compiler can eliminate *all* `assert` statements in the program of Figure 4, if the program is run by principal `"User"`.