A Calculus for Flow-Limited Authorization

Corrected version: August 30th, 2017*

Owen Arden
Department of Computer Science
Cornell University
owen@cs.cornell.edu

Andrew C. Myers
Department of Computer Science
Cornell University
andru@cs.cornell.edu

Abstract—Real-world applications routinely make authorization decisions based on dynamic computation. Reasoning about dynamically computed authority is challenging. Integrity of the system might be compromised if attackers can improperly influence the authorizing computation. Confidentiality can also be compromised by authorization, since authorization decisions are often based on sensitive data such as membership lists and passwords. Previous formal models for authorization do not fully address the security implications of permitting trust relationships to change, which limits their ability to reason about authority that derives from dynamic computation. Our goal is a way to construct dynamic authorization mechanisms that do not violate confidentiality or integrity.

We introduce the Flow-Limited Authorization Calculus (FLAC), which is both a simple, expressive model for reasoning about dynamic authorization and also an information flow control language for securely implementing various authorization mechanisms. FLAC combines the insights of two previous models: it extends the Dependency Core Calculus with features made possible by the Flow-Limited Authorization Model. FLAC provides strong end-to-end information security guarantees even for programs that incorporate and implement rich dynamic authorization mechanisms. These guarantees include noninterference and robust declassification, which prevent attackers from influencing information disclosures in unauthorized ways. We prove these security properties formally for all FLAC programs and explore the expressiveness of FLAC with several examples.

I. INTRODUCTION

Authorization mechanisms are critical components in all distributed systems. The policies enforced by these mechanisms constrain what computation may be safely executed, and therefore an expressive policy language is important. Expressive mechanisms for authorization have been an active research area. A variety of approaches have been developed, including authorization logics [1], [2], [3], often implemented with cryptographic mechanisms [4], [5]; role-based access control (RBAC) [6]; and trust management [7], [8], [9].

However, the security guarantees of authorization mechanisms are usually analyzed using formal models that abstract away the computation and communication performed by the system. Developers must take great care to faithfully preserve the (often implicit) assumptions of the model, not only when implementing authorization mechanisms, but also when employing them. Simplifying abstractions can help extract formal security guarantees, but abstractions can also obscure the challenges of implementing and using an abstraction securely. This disconnect between abstraction and implementation can lead to vulnerabilities and covert channels that allow attackers to leak or corrupt information.

A common blind spot in many authorization models is confidentiality. Most models cannot express authorization policies that are confidential or are based on confidential data. Real systems, however, use confidential data for authorization all the time: users on social networks receive access to photos based on friend lists, frequent fliers receive tickets based on credit card purchase histories, and doctors exchange patient data while keeping doctor–patient relationships confidential. While many models can ensure, for instance, that only friends are permitted to access a photo, few can say anything about the secondary goal of preserving the confidentiality of the friend list. Such authorization schemes may fundamentally require some information to be disclosed, but failing to detect these disclosures can lead to unintentional leaks.

Authorization without integrity is meaningless, so formal models are typically better at enforcing integrity. However, many formal models make unreasonable or unintuitive assumptions about integrity. For instance, in many models (e.g., [1], [2], [7]) authorization policies either do not change or change only when modified by a trusted administrator. This is a reasonable assumption in centralized systems where such an administrator will always exist, but in decentralized systems, there may be no single entity that is trusted by all other entities. Even in centralized systems, administrators must be careful when performing updates based on partially trusted information, since malicious users may try to use the administrator to carry out an attack on their behalf. Unfortunately, existing models offer little help to administrators that need to reason about how attackers may have influenced security-critical update operations.

Developers need a better programming model for implementing expressive dynamic authorization mechanisms. Errors that undermine the security of these mechanisms are common [10], so we want to be able to verify their security. We argue that information flow control is a lightweight, useful tool for building secure authorization mechanisms. Using information flow control is attractive since it offers compositional, end-
to-end security guarantees. However, applying information flow control to these mechanisms in a meaningful way requires building on a theory that integrates authority and information security. In this work, we show how to embed such a theory into a programming model, so that dynamic authorization mechanisms—as well as the programs that employ them—can be statically verified.

Approaching the verification of dynamic authorization mechanisms from this perspective is attractive for two reasons. First, it gives a model for building secure authorization mechanisms by construction rather than verifying them after the fact. This model offers programmers insight into the sometimes subtle interaction between information flow and authorization, and helps programmers address problems early, during the design process. Second, it addresses a core weakness lurking at the heart of existing language-based security schemes: that the underlying policies may change in a way that breaks security. By statically verifying the information security of dynamic authorization mechanisms, we expand the real-world scenarios in which language-based information flow control is useful and strengthen its security guarantees.

We demonstrate that such an embedding is possible by presenting a core language for authorization and information flow control, called the Flow-Limited Authorization Calculus (FLAC). FLAC is a functional language for designing and verifying decentralized authorization protocols. FLAC is inspired by the Polymorphic Dependency Core Calculus [2] (DCC).\(^1\) Abadi develops DCC as an authorization logic, but DCC is limited to static trust relationships defined externally to DCC programs by a lattice of principals. FLAC supports dynamic authorization by building on the Flow-Limited Authorization Model (FLAM) [12], which unifies reasoning about authority, confidentiality, and integrity. Furthermore, FLAC is a language for information flow control. It uses FLAM’s principal model and FLAM’s logical reasoning rules to define an operational model and type system for authorization computations that preserve information security.

The types in a FLAC program can be considered propositions [13] in an authorization logic, and the programs can be considered proofs that the proposition holds. Well-typed FLAC programs are not only proofs of authorization, but also proofs of secure information flow, ensuring the confidentiality and integrity of authorization policies and of the data those policies depend upon.

FLAC is useful from a logical perspective, but also serves as a core programming model for real language implementations. Since FLAC programs can dynamically authorize computation and flows of information, FLAC applies to more realistic settings than previous authorization logics. Thus FLAC offers more than a type system for proving propositions—FLAC programs do useful computation.

This paper makes the following contributions.

- We define FLAC, a language, type system, and semantics for dynamic authorization mechanisms with strong information security:
  - Programs in low-integrity contexts exhibit noninterference, ensuring attackers cannot leak or corrupt information, and cannot subvert authorization mechanisms.
  - Programs in higher-integrity contexts exhibit robust declassification, ensuring attackers cannot influence authorized disclosures of information.
- We present two authorization mechanisms implemented in FLAC, commitment schemes and bearer credentials, and demonstrate that FLAC ensures the programs that use these mechanisms preserve the desired confidentiality and integrity properties.

We have organized our discussion of FLAC as follows. Section II introduces commitment schemes and bearer credentials, two examples of dynamic authorization mechanisms we use to explore the features of FLAC. Section III reviews the FLAM principal lattice [12], and Section IV defines the FLAC language and type system. FLAC implementations of the dynamic authorization examples are presented in Section V, and their properties are examined. Section VI explores aspects of FLAC’s proof theory, and Section VII discusses semantic security guarantees of FLAC programs, including noninterference and robust declassification. We explore related work in Section VIII and conclude in Section IX.

## II. Dynamic Authorization Mechanisms

Dynamic authorization is challenging to implement correctly since authority, confidentiality, and integrity interact in subtle ways. FLAC helps programmers securely implement both authorization mechanisms and code that uses them. FLAC types support the definition of compositional security abstractions, and vulnerabilities in the implementations of these abstractions are caught statically. Further, the guarantees offered by FLAC simplify reasoning about the security properties of these abstractions.

We illustrate the usefulness and expressive power of FLAC using two important security mechanisms: commitment schemes and bearer credentials. We show in Section V that these mechanisms can be implemented using FLAC, and that their security goals are easily verified in the context of FLAC.

### A. Commitment schemes

A commitment scheme [14] allows one party to give another party a “commitment” to a secret value without revealing the value. The committing party may later reveal the secret in a way that convinces the receiver that the revealed value is the value originally committed.

Commitment schemes provide three essential operations: commit, receive, and open. Suppose \( p \) wants to commit to a value to principal \( q \). First, \( p \) applies commit to the value and provides the result to \( q \). Next, \( q \) applies receive to the committed value. Finally, when \( p \) wishes to reveal the value, \( p \) applies the open operation to the received value, permitting \( q \) to learn it.
A commitment scheme must have several properties in order to be secure. First, $q$ should not be able to receive a value that hasn’t been committed by $p$, since this could allow $q$ to manipulate $p$ to open a value it had not committed to. Second, $q$ should not learn any secret of $p$ that has not been opened by $p$. Third, $p$ should not be able to open a different value than the one received by $q$.

One might wonder why a programmer would bother to create high-level implementations of operations like commit, receive, and open. Why not simply treat these as primitive operations and give them type signatures so that programs using them can be type-checked with respect to those signatures? The answer is that an error in a type signature could lead to a serious vulnerability. Therefore, we want more assurance that the type signatures are correct. Implementing such operations in FLAC is often easy and ensures that the type signature is consistent with a set of assumptions about existing trust relationships and the information flow context the operations are used within. These FLAC-based implementations serve as language-based models of the security properties achieved by implementations that use cryptography or trusted third parties.

B. Bearer credentials with caveats

A bearer credential is a capability that grants authority to any entity that possesses it. Many authorization mechanisms used in distributed systems employ bearer credentials in some form. Browser cookies that store session tokens are one example: after a website authenticates a user’s identity, it gives the user a token to use in subsequent interactions. Since it is infeasible for attackers to guess the token, the website grants the authority of the user to any requests that include the token.

Bearer credentials create an information security conundrum for authorization mechanisms. Though they efficiently control access to restricted resources, they create vulnerabilities and introduce covert channels when used incorrectly. For example, suppose Alice shares a remotely-hosted photo with her friends by giving them a credential to access the photo. Giving a friend such a credential doesn’t disclose their friendship, but each friend that accesses the photo implicitly discloses the friendship to the hosting service. Such covert channels are pervasive, both in classic distributed authorization mechanisms like SPKI/SDSI [4], as well as in more recent ones like Macaroons [5].

Bearer credentials can also lead to vulnerabilities if they are leaked. If an attacker obtains a credential, it can exploit the authority of the credential. Thus, to limit the authority of a credential, approaches like SPKI/SDSI and Macaroons provide constrained delegation in which a newly issued credential attenuates the authority of an existing one by adding caveats. Caveats require additional properties to hold for the bearer to be granted authority. Session tokens, for example, might have a caveat that restricts the source IP address or encodes an expiration time. As pointed out by Birgisson et al. [5], caveats themselves can introduce covert channels if the properties reveal sensitive information.

FLAC is an effective framework for reasoning about bearer credentials with caveats since it captures the flow of credentials in programs as well as the sensitivity of the information the credentials and caveats derive from. We can reason about credentials and the programs that use them in FLAC with an approach similar to that used for commitment schemes. That we can do so in a straightforward way is somewhat remarkable: prior formalizations of credential mechanisms (e.g., [5], [15], [16]) usually do not consider confidentiality nor provide end-to-end guarantees about credential propagation.

III. THE FLAM PRINCIPAL LATTICE

Like many models, FLAM uses principals to represent the authority of all entities relevant to a system. However, FLAM’s principals and their algebraic properties are richer than in most models, so we briefly review the FLAM principal model and notation. Further details are found in the earlier paper [12].

Primitive principals such as Alice, Bob, etc., are represented as elements of a (potentially infinite) set of names $\mathcal{N}$. In addition, FLAM uses $\top$ to represent a universally trusted principal and $\bot$ to represent a universally untrusted principal. The combined authority of two principals, $p$ and $q$, is represented by the conjunction $p \land q$, whereas the authority of either $p$ or $q$ is the disjunction $p \lor q$.

Unlike principals in other models, FLAM principals also represent information flow policies. The confidentiality of principal $p$ is represented by the principal $p^{\rightarrow}$, called $p$’s confidentiality projection. It denotes the authority necessary to learn anything $p$ can learn. The integrity of principal $p$ is represented by $p^{\leftarrow}$, called $p$’s integrity projection. It denotes the authority to influence anything $p$ can influence.

All authority may be represented as some combination of confidentiality and integrity. For instance, principal $p$ is equivalent to the conjunction $p^{\rightarrow} \land p^{\leftarrow}$ and in fact any FLAM principal can be written $p^{\rightarrow} \land q^{\leftarrow}$ for some $p$ and $q$. The closure of the set of names $\mathcal{N}$ plus $\top$ and $\bot$ under the operators $\land, \lor, \leftarrow, \rightarrow$ forms a lattice $\mathcal{L}$ ordered by an acts-for relation $\Rightarrow$, defined by the inference rules in Figure 1. We write operators $\leftarrow, \rightarrow$ with higher precedence than $\land, \lor$; for instance, $p^{\land q^{\leftarrow}}$ is equal to $p^{\rightarrow} \land (p^{\leftarrow} \lor q^{\leftarrow})$. Projections distribute over $\land$ and $\lor$ so, for example, $(p \land q)^{\leftarrow} = (p^{\leftarrow} \land q^{\leftarrow})^{\leftarrow}$. The confidentiality and integrity authority of principals are disjoint, so the confidentiality projection of an integrity projection is $\bot$ and vice-versa: $(p^{\rightarrow})^{\land} = \bot = (p^{\land})^{\rightarrow}$.

An advantage of this model is that secure information flow can be defined in terms of authority. An information flow policy $q$ is at least as restrictive as a policy $p$ if $q$ has at least the confidentiality authority $p^{\rightarrow}$ and $p$ has at least the integrity

2Using $\mathcal{N}$ as the set of all names is convenient in our formal calculus, but a general-purpose language based on FLAC may wish to dynamically allocate names at runtime. Since knowing or using a principal’s name holds no special privilege in FLAC, this presents no fundamental difficulties. To use dynamically allocated principals in type signatures, however, the language’s type system should support types in which principal names may be existentially quantified.

3FLAM defines an additional set of operators called ownership projections, which we omit here to simplify our presentation.
authority $q^-$. This relationship between the confidentiality and integrity of $p$ and $q$ reflects the usual duality seen in information flow control [17]. As in [12], we use the following shorthand for relating principals by policy restrictiveness:

$$p \subseteq q \triangleq (p^- \land q^-) \supseteq (q^- \land p^-)$$
$$p \sqcup q \triangleq (p \land q)^- \supseteq (p \lor q)^-$$
$$p \sqcap q \triangleq (p \lor q)^- \supseteq (p \land q)^-$$

Thus, $p \subseteq q$ indicates the direction of secure information flow: from $p$ to $q$. The information flow join $p \sqcup q$ is the least restrictive principal that both $p$ and $q$ flow to, and the information flow meet $p \sqcap q$ is the most restrictive principal that flows to both $p$ and $q$.

Finally, in FLAC, the ability to “speak for” another principal is an integrity relationship between principals. This makes sense intuitively, because speaking for another principal influences that principal’s trust relationships and information flow policies. FLAC defines the voice of a principal $p$, written $\nabla(p)$, as the integrity necessary to speak for that principal. Given a principal expressed in normal form as $(q^- \land r^-)$, the voice of that principal is

$$\nabla(q^- \land r^-) \triangleq q^- \land r^-$$

For example, the voice of Alice, $\nabla(Alice)$, is $Alice^-$. The voice of Alice’s confidentiality $\nabla(Alice^-)$ is also $Alice^-$.

IV. FLOW-LIMITED AUTHORIZATION CALCULUS

FLAC uses information flow to reason about the security implications of dynamically computed authority. Like previous information-flow type systems [18], FLAC incorporates types for reasoning about information flow, but FLAC’s type system goes further by using Flow-Limited Authorization [12] to ensure that principals cannot use FLAC programs to exceed their authority, or to leak or corrupt information. FLAC is based on DCC [2], but unlike DCC, FLAC supports reasoning about authority deriving from the evaluation of FLAC terms. In contrast, all authority in DCC derives from trust relationships defined by a fixed, external lattice of principals. Thus, using an approach based on DCC in systems where trust relationships change dynamically could introduce vulnerabilities like delegation loopholes, probing and poaching attacks, and authorization side channels [12].

Figure 2 defines the FLAC syntax; evaluation contexts [19] are defined in Figure 3. The core operational semantics in Figure 4 is mostly standard except for `assume` terms, discussed below.

The core FLAC type system is presented in Figure 5. FLAC typing judgments have the form $\Pi; \Gamma; pc \vdash e : s$. The delegation context, $\Pi$, contains a set of labeled dynamic trust relationships $\langle p \triangleright q \mid \ell \rangle$ where $p \triangleright q$ (read as “$p$ acts for $q$”) is a delegation from $q$ to $p$, and $\ell$ is the confidentiality and integrity of that information. The typing context, $\Gamma$, is a map from variables to types, and $pc$ is the program counter label, a FLAC principal representing the confidentiality and integrity of control flow. The type system makes frequent use of judgments adapted from FLAC’s inference rules [12].

---

4In normal form, a principal is the conjunction of a confidentiality principal and an integrity principal. See [12] for details.

---
These rules, adapted to FLAC, are presented in Figure 6.5

Since FLAC is a pure functional language, it might seem odd for FLAC to have a label for the program counter; such labels are usually used to control implicit flows through assignments (e.g., in [20], [21]). The purpose of FLAC's pc label is to control a different kind of side effect: changes to the delegation context. \( \Pi \).5 In order to control what information can influence whether a new trust relationship is added to the delegation context, the type system tracks the confidentiality and security of control flow. Viewed as an authorization logic, FLAC's type system has the unique feature that it expresses deduction constrained by an information flow context. For instance, if we have \( \psi \stackrel{\cdot}{\Rightarrow} \) and \( \varphi \) then (via APP) we may derive \( \psi \) in a context with integrity \( p \Rightarrow \), but not in contexts that don't flow to \( p \Rightarrow \). This feature offers needed control over how principals may apply existing facts to derive new facts.

Many FLAC terms are standard, such as pairs \((e_1, e_2)\), projections \(proj_j\), variants \( inj_j\), polymorphic type abstraction, \( \Lambda X. e \), and case expressions. Function abstraction, \( \lambda(x : s)[pc]. e \), includes a \( pc \) label that constrains the information flow context in which the function may be applied. The rule APP ensures that function application respects these policies, requiring that the robust FLAM judgment \( \Pi; pc; pc \vdash pc \subseteq pc' \) holds. This judgment ensures that the current program counter label, \( pc \), flows to the function label, \( pc' \).

Branching occurs in case expressions, which conditionally evaluate one of two expressions. The rule CASE ensures that both expressions have the same type and thus the same protection level. The premise \( \Pi; pc \vdash pc \leq s \) ensures that this type protects the current \( pc \) label.7

\[ e \rightarrow e' \]

\[ \text{[E-APP]} \quad (\lambda(x : s)[pc]. e) \, v \rightarrow e[x \mapsto v] \]

\[ \text{[E-TAPP]} \quad (\Lambda X. e) \, s \rightarrow e[X \mapsto s] \]

\[ \text{[E-UNPAIR]} \quad \text{proj}_j \, (v_1, v_2) \rightarrow v_i \]

\[ \text{[E-CASE]} \quad \text{(case } (\text{inj}_1 \, v) \text{ of } \text{inj}_1 (x). \, c_1 \mid \text{inj}_2 (x). \, c_2) \rightarrow \text{e}(x \mapsto v) \]

\[ \text{[E-BINDM]} \quad \text{bind } x = (\eta \ell \, v) \in e \rightarrow e[x \mapsto v] \]

\[ \text{[E-ASSUME]} \quad \text{assume } (p \Rightarrow q) \in e \rightarrow e \text{ where } (p \Rightarrow q) \]

\[ \text{[E-EVAL]} \quad e \rightarrow e' \]

\[ E[e] \rightarrow E[e'] \]

Fig. 4: FLAC operational semantics

Like DCC, FLAC uses monadic operators to track dependencies. The monadic unit term \( (\eta \ell \, v) \) (UNITM) says that a value \( v \) of type \( s \) is protected at level \( \ell \). This protected value has the type \( \ell \) says \( s \), meaning that it has the confidentiality and integrity of principal \( \ell \). Computation on protected values must occur in a protected context (“in the monad”), expressed using a monadic bind term. The typing rule BINDM ensures that the result of the computation protects the confidentiality and integrity of protected values. For instance, the expression \( \text{bind } x = (\eta \ell \, v) \in (\eta \ell' \, x) \) is only well-typed if \( \ell' \) protects...
values with confidentiality and integrity $\ell$. Since case expressions may use the variable $x$ for branching, BINDM raises the $pc$ label to $pc \sqcup \ell$ to conservatively reflect the control-flow dependency.

Protection levels are defined by the set of inference rules in Figure 8, adapted from [22]. Expressions with unit type (P-UNIT) do not propagate any information, so they protect information at any $\ell$. Product types protect information at $\ell$ if both components do (P-PAIR). Function types protect information at $\ell$ if the return type does (P-FUN), and polymorphic types protect information at whatever level the abstracted type does (P-TFUN). If a type $s$ already protects information at $\ell$, then $\ell'$ $\text{says}$ $s$ still does (P-LBL1). Finally, if $\ell$ flows to $\ell'$, then $\ell'$ $\text{says}$ $s$ protects information at $\ell$ (P-LBL2).

Most of the novelty of FLAC lies in its delegation values and assume terms. These terms enable expressive reasoning about authority and information flow control. A delegation value serves as evidence of trust. For instance, the term $(p \triangleright q)$, read "$p$ acts for $q$", is evidence that $q$ trusts $p$. Delegation values have acts-for types; $(p \triangleright q)$ has type $(p \triangleright q)$.

The assume term enables programs to use evidence securely to create new flows between protection levels. In the typing context $\emptyset; x: p \rightsquigarrow$ $s$; $q^{\sim}$ (i.e., $\emptyset = \emptyset$, $\Gamma = x: p \rightsquigarrow$ $s$, and $pc = q^{\sim}$), the following expression is not well typed:

$$\text{bind } x' = x \text{ in } (\eta_{q^{\sim}} x')$$

since $p^{\sim}$ does not flow to $q^{\sim}$, as required by the premise $\Pi; pc$ $\vdash \ell \leq s$ in rule BINDM. Specifically, we cannot derive $\Pi; pc \vdash p^{\sim} \leq q^{\sim}$ $\text{says}$ $s$ since P-LBL2 requires the FLAM judgment $\Pi; q^{\sim}; q^{\sim} \vdash p^{\sim} \sqsubseteq q^{\sim}$ to hold.

However, the following expression is well typed:

$$\text{assume } (p^{\sim} \triangleright q^{\sim}) \text{ in bind } x' = x \text{ in } (\eta_{q^{\sim}} x')$$

The difference is that the assume term adds a trust relationship, represented by an expression with an acts-for type, to the delegation context. In this case, the expression $(p^{\sim} \triangleright q^{\sim})$ adds a trust relationship that allows $p^{\sim}$ to flow to $q^{\sim}$. This is secure since $pc = q^{\sim}$, meaning that only principals with integrity $q^{\sim}$ have influenced the computation. With $(p^{\sim} \triangleright q^{\sim} | q^{\sim})$ in the delegation context, added via the ASSUME rule, the premises of BINDM are now satisfied, so the expression type-checks.

Creating a delegation value requires no special privilege because the type system ensures only high-integrity delegations are used as evidence that enable new flows. Using low-integrity evidence for authorization would be insecure since attackers could use delegation values to create new flows that reveal secrets or corrupt data. The premises of the ASSUME rule ensure the integrity of dynamic authorization computations that produce values like $(p^{\sim} \triangleright q^{\sim})$ in the example above.\(^9\)

The second premise, $\Pi; pc; pc \vdash p \triangleright q$, requires that the $pc$ has enough integrity to be trusted by $q$, the principal whose security is affected. For instance, to make the assumption $p \triangleright q$, the evidence represented by the term $e$ must have at least the integrity of the voice of $q$, written $\nabla(q)$. Since the $pc$ bounds the restrictiveness of the dependencies of $e$, this ensures that only information with integrity $\nabla(q)$ or higher may influence the evaluation of $e$. The third premise, $\Pi; pc \vdash \nabla(p^{\sim}) \triangleright \nabla(q^{\sim})$, ensures that principal $p$ has sufficient integrity to be trusted to enforce $q^{\sim}$’s confidentiality, $q^{\sim}$. This premise means that $q$ permits data to be relabeled from $q^{\sim}$ to $p^{\sim}$.\(^{10}\)

Assumption terms evaluate to where expressions (rule E-ASSUME). To simplify the formalization, these expressions are not part of the source language but are generated by the evaluation rules. The term $e$ where $v$ records that $e$ is evaluated in a context that includes the delegation $v$. The rule WHERE gives a typing rule for where terms; though similar to

\[^9\]These premises are related to the robust FLAM rule LIFT.
\[^{10}\]More precisely, it means that the voice of $q^{\sim}$’s confidentiality, $\nabla(q^{\sim})$, permits data to be relabeled from $q^{\sim}$ to $p^{\sim}$. Recall that $\nabla(q^{\sim})$ is just Alice's integrity projection: $\text{Alice}^{q^{\sim}}$. 
ASSUME, it requires only that there exist a sufficiently trusted label pc such that subexpression e type-checks. In the proofs in Section VII, we choose pc using the typing judgment of the source-level assume that generates the where term.

Figure 7 presents evaluation rules for where terms. These terms are simply a bookkeeping mechanism: these evaluation rules simply record and maintain the authorization evidence used to justify new flows of information that occur during the evaluation of a FLAC program. The rules are designed to treat where values like the value they enclose. For instance, applying a where term (rule W-APP) simply moves the value it is applied to inside the where term. If the where term was wrapping a lambda expression, then it may now be applied via APP. Otherwise, further reduction steps via W-APP may be necessary.

V. EXAMPLES REVISITED

We can now implement our examples from Section II in FLAC. Using FLAC ensures that authority and information flow assumptions are explicit, and that programs using these abstractions are secure with respect to those assumptions. In this section, we discuss at a high level how FLAC types help enforce specific end-to-end security properties for commitment schemes and bearer credentials. Section VII formalizes the semantic security properties of all well-typed FLAC programs.

A. Commitment Schemes

Figure 9 contains the essential operations of a one-round commitment scheme—commit, receive, and open—implemented in FLAC. Typically, a principal p commits to a value and sends it to q, who receives it. Later, p opens the value, revealing it to q. The commit operation takes a value of any type (hence ∀X) with confidentiality p→ and produces a value with confidentiality and integrity p. In other words, p endorses [24] the value to have integrity p→.

Attacker should not be able to influence whether principal p commits to a particular value. The pc constraint on commit ensures that only principal p and principals trusted with at least p's integrity, p→, may apply commit to a value. Furthermore, if the programmer omitted this constraint or instead chose ⊥→, say, then commit would be rejected by the type system. Specifically, the assume term would not type-check via rule ASSUME since the pc does not act for ∇(p→) = p→.

Next, principal q accepts a committed value from p using the receive operation. The receive operation endorses the value with q's integrity, resulting in a value at p ∧ q→, the confidentiality of p and the integrity of both p and q.

As with the commit operation, FLAC ensures that receive satisfies important information security properties. Other principals, including p, should not be able to influence which values q receives—otherwise an attacker could use receive to subvert q's integrity, using it to endorse arbitrary values. The pc constraint on receive ensures in this case that only q may apply receive. Furthermore, the type of x requires received values to have the integrity of p. Errors in either of these constraints would result in a typing error, either due to ASSUME as before, or due to BINDM, which requires that p must flow to p ∧ q→.

Additionally, receive accepts committed values with confidentiality at most p→. This constraint ensures that q does not receive values from p that might depend on q's secrets: unopened commitments, for example. In cryptographic protocols, this property is usually called non-malleability [26], and is important for scenarios in which security depends on the independence of values. Consider a sealed-bid auction where participants submit their bids via commitment protocols. Suppose that q commits a bid b, protected by label q. Then p could theoretically influence a computation that computes a value b + 1 with label p ∧ q→ since that label protects

\[\text{commit:}\forall X. p \vdash X \quad \text{p says X}\]
\[\text{commit} =\]
\[\Lambda X. (\lambda x : p \rightarrow X)[p→].\]
\[\text{assume } \langle \bot \rightarrow p \rightarrow X \rangle \text{ in bind } x' = x \text{ in } (\eta_p x').\]
\[\text{receive:}\forall X. p \vdash X \quad q \rightarrow p \land q→ \text{ says X}\]
\[\text{receive} =\]
\[\Lambda X. (\lambda x : p \rightarrow X)[q→].\]
\[\text{assume } \langle p→ \rightarrow 1 \rightarrow X \rangle \text{ in bind } x' = x \text{ in } (\eta_p \land q→ x').\]
\[\text{open:}\forall X. p \land q→ \text{ says X}\]
\[\text{open} =\]
\[\Lambda X. (\lambda x : p \land q→ \rightarrow X)[\eta(p→)].\]
\[\text{assume } \langle \eta(q→) \rightarrow \eta(p→) \rangle \text{ in assume } \langle q→ \rightarrow p→ \rangle \text{ in bind } x' = x \text{ in } (\eta_p \land q x').\]
information at \(q^{-}\), but only has \(p^{-}\) integrity. If \(q\) received values from \(p\) that could depend on \(q\)'s secrets, then \(p\) could outbid \(q\) by 1 without ever learning the value of \(b\).

Finally, open reveals a committed value to \(q\) by relabeling a value from \(p \land q^{-}\) to \(p^{-} \land q\), which is readable by principal \(q\) but retains the integrity of both \(p\) and \(q\). Since open accepts a value protected by the integrity of both \(p\) and \(q\) and returns a value with the same integrity, the opened value must have been previously committed by \(p\) and received by \(q\). Since the open operation reveals a value with confidentiality \(p^{-}\), it should only be invoked by principals that are trusted to speak for \(p^{-}\). Otherwise, \(q\) could open \(p\)'s commitments. Hence, the \(pc\) label of open is \(\nabla(p^{-})\). For \(p = Alice\), say, the \(pc\) label would be \(Alice^{-}\). FLAC ensures these constraints are specified correctly; otherwise, open’s implementation could not produce a value with label \(p^{-} \land q\).

The implementation requires two assume terms. The outer term establishes that principals speaking for \(q^{-}\) also speak for \(p^{-}\) by creating an integrity relationship between their voices. With this relationship in place, the inner term may reveal the commitment to \(q\).\(^{12}\)

In DCC, functions are not annotated with \(pc\) labels and may be applied in any context. So a DCC function analogous to open might have type

\[
dcc\_open : \forall X. p \land q^{-} \text{ says } X \rightarrow p^{-} \land q \text{ says } X
\]

However, \(dcc\_open\) would not be appropriate for a commitment scheme since any principal could use it to relabel information from \(p\)-confidential \((p^{-})\) to \(q\)-confidential \((q^{-})\).

To simplify the presentation of our commitment scheme operations, we make the assumption that \(q\) only receives one value. Therefore, \(p\) can only open one value, since only one value has been given the integrity of both \(p\) and \(q\). A more general scheme can be achieved by pairing each committed value with a public identifier that is endorsed along with the value, but remains public. If \(q\) refuses to receive more that one commitment with the same identifier, \(p\) will be unable to open two commitments with the same value since it cannot create a pair that has the integrity of both \(p\) and \(q\), even if \(p\) has multiple committed values (with different identifiers) to choose from. We present the simpler one-round commitment scheme above since it captures the essential information security properties of commitment while avoiding the tedious digression of defining encodings for numeric values and numeric comparisons.

The real power of FLAC is that the security guarantees of well-typed FLAC functions like those above are compositional. The FLAC type system ensures the security of both the functions themselves and the programs that use them. For instance, the code should be rejected because it would permit \(q\) to open \(p\)'s commitments:

\[
\lambda(x : p \land q^{-} \text{ says } X)[q^{-}], \text{ assume } \langle q \triangleright p \rangle \text{ in open } x
\]

FLAC’s guarantees make it possible to state general security properties of all programs that use the above commitment scheme, even if those programs are malicious. For example, suppose we have \(pc_{p} = \nabla(p), pc_{q} = \nabla(q)\), and

\[
\Gamma_{cro} = \text{commit, receive, open, } x : p^{-} \rightarrow s, y : p \land q^{-} \text{ says } s
\]

Intuitively, \(pc_{p}\) and \(pc_{q}\) are execution contexts under the control of \(p\) or \(q\), respectively. \(\Gamma_{cro}\) is a typing context for programs using the commitment scheme.\(^{14}\) The variable \(x\) represents an uncommitted value with \(p\)'s confidentiality, whereas \(y\) is a committed value. Since we are interested in properties that hold for all principals \(p\) and \(q\), we want the properties to hold in an empty delegation context: \(\Pi = \emptyset\).

Below, we omit the delegation context altogether for brevity.

Using results presented in Section VII, we can prove that:

- \(q\) cannot receive a value that hasn’t been committed.
  - For any \(e\) and \(s'\) such that \(\Gamma_{cro}; pc_{q} \vdash e : p \land q^{-}\) says \(s'\), result of \(e\) is independent of \(x\); specifically, for any \(v_{1}\) and \(v_{2}\), if \(e[x \mapsto v_{1}] \rightarrow^{*} v'_{1}\) and \(e[x \mapsto v_{2}] \rightarrow^{*} v'_{2}\), then \(v'_{1} = v'_{2}\).
- \(q\) cannot learn a value that hasn’t been opened.
  - For any \(e, \ell, \) and \(s'\) such that \(\Gamma_{cro}; pc_{q} \vdash e : \ell \land q^{-}\) says \(s'\), then the result of \(e\) is independent of \(x\) and \(y\).
- \(p\) cannot open a value that hasn’t been received.
  - For any \(e\) such that \(\Gamma_{cro}; pc_{p} \vdash e : p^{-} \land q\) says \(s'\), then the result of \(e\) is independent of \(x\).

For the first two properties, we consider programs using our commitment scheme that \(q\) might invoke, hence we consider FLAC programs that type-check in the \(\Gamma_{cro}; pc_{q}\) context. In the first property, we are concerned with programs that produce values protected by policy \(p \land q^{-}\). Since such programs produce values with the integrity of \(p\), we want to ensure that no program exists that enables \(q\) to obtain a value with \(p\)'s integrity that depends on \(x\), which is a value without \(p\)'s integrity. The second property concerns programs that produces values at \(\ell \land q^{-}\) for any \(\ell\); these are values readable by \(q\). Therefore, we want to ensure that no program exists that enables \(q\) to produce such a value that depends on \(x\) or \(y\), which are not readable by \(q\).

The final property considers programs that \(p\) might invoke to produce values at \(p^{-} \land q\), thus we consider FLAC programs that type-check in the \(\Gamma_{cro}; pc_{p}\) context. Here, we want to ensure that no program invoked by \(p\) can produce a value at \(p^{-} \land q\) that depends on \(x\), an unreceived value. Complete proofs of these properties are found in Appendix B.

B. Bearer Credentials

We can also use FLAC to implement bearer credentials, our second example of a dynamic authorization mechanism. We

\(^{12}\) i.e., it satisfies the \text{ASSUME} premise \(\Pi; pc ; pc \triangleright \nabla(p^{-}) \triangleright \nabla(q^{-})\).

\(^{14}\) For presentation purposes, we have omitted the types of \text{commit, receive, and open} in \(\Gamma_{cro}\). Their types are as defined previously.
represent a bearer credential with authority $k$ in FLAC as a term with the type

$$\forall X. k^{-} \text{ says } X \xrightarrow{pc} k^{-} \text{ says } X$$

which we abbreviate as $k^{-} \xrightarrow{pc} k^{-}$. These terms act as bearer credentials for a principal $k$ since they may be used as a proxy for $k$’s confidentiality and integrity authority. Recall that $k^{-} = k^{-} \land \bot^{-}$ and $k^{-} = k^{-} \land \bot^{-}$. Then secrets protected by $k^{-}$ can be declassified to $\bot^{-}$, and untrusted data protected by $\bot^{-}$ can be endorsed to $k^{-}$. Thus this term wields the full authority of $k$, and if $pc = \bot^{-}$, the credential may be used in any context—any “bearer” may use it. From such credentials, more restricted credentials can be derived. For example, the credential $k^{-} \xrightarrow{pc} \bot^{-}$ grants the bearer authority to declassify $k$-confidential values, but no authority to endorse values.

We postpone an in-depth discussion of terms with types of the form $k^{-} \xrightarrow{pc} k^{-}$ until Section VI-B, but it is interesting to note that an analogous term in DCC is only well-typed if $k$ is equivalent to $\bot$. This is because the function takes an argument with $k^{-}$ confidentiality and no integrity, and produces a value with $k^{-}$ integrity and no confidentiality. Suppose $L$ is a security lattice used to type-check DCC programs with suitable encodings for $k$’s confidentiality and integrity. If a DCC term has a type analogous to $k^{-} \Rightarrow k^{-}$, then $L$ must have the property $k^{-} \sqsubseteq \bot$ and $\bot \sqsubseteq k^{-}$. This means that $k$ has no confidentiality and no integrity. That FLAC terms may have this type for any principal $k$ makes it straightforward to implement bearer credentials and demonstrates a useful application of FLAC’s expressiveness.

The $pc$ of a credential $k^{-} \xrightarrow{pc} k^{-}$ acts as a sort of caveat: it restricts the information flow context in which the credential may be used. We can add more general caveats to credentials by wrapping them in lambda terms. To add a caveat $\phi$ to a credential with type $k^{-} \xrightarrow{pc} k^{-}$, we use a wrapper:

$$\lambda(x)(k^{-} \xrightarrow{pc} k^{-})(pc), \Lambda X. \lambda(y; \phi)(pc), x X$$

which gives us a term with type

$$\forall X. \phi \xrightarrow{pc} k^{-} \text{ says } X \xrightarrow{pc} k^{-} \text{ says } X$$

This requires a term with type $\phi$ (in which $X$ may occur) to be applied before the authority of $k$ can be used. Similar wrappers allow us to chain multiple caveats; i.e., for caveats $\phi_{1} \ldots \phi_{n}$, we obtain the type

$$\forall X. \phi_{1} \xrightarrow{pc} \ldots \phi_{n} \xrightarrow{pc} \phi_{n} k^{-} \text{ says } X \xrightarrow{pc} k^{-} \text{ says } X$$

which abbreviates to

$$k^{-} \xrightarrow{\phi_{1} \ldots \phi_{n} \xrightarrow{pc}} k^{-}$$

Like any other FLAC terms, credentials may be protected by information flow policies. So a credential that should only be accessible to Alice might be protected by the type $Alice^{-} \text{ says } (k^{-} \xrightarrow{pc} k^{-})$. This confidentiality policy ensures the credential cannot accidentally be leaked to an attacker. A further step might be to constrain uses of this credential so that only Alice may invoke it to relabel information. If we require $pc = Alice^{-}$, this credential may only be used in contexts trusted by Alice: $Alice^{-} \text{ says } (k^{-} \xrightarrow{\phi_{Alice^{-}}} k^{-})$.

A subtle point about the way in which we construct caveats is that the caveats are polymorphic with respect to $X$, the same type variable the credential ranges over. This means that each caveat may constrain what types $X$ may be instantiated with. For instance, suppose $isEduc$ is a predicate for educational films; it holds (has a proof term with type $isEduc\ X$) for types like $Bio$ and $Doc$, but not $RomCom$. Adding $isEduc\ X$ as a caveat to a credential would mean that the bearer of the credential could use it to access biographies and documentaries, but could not use it to access romantic comedies. Since no term of type $isEduc\ RomCom$ could be applied, the bearer could only satisfy $isEduc$ by instantiating $X$ with $Bio$ or $Doc$. Once $X$ is instantiated with $Bio$ or $Doc$, the credential cannot be used on a $RomCom$ value. Thus we have two mechanisms for constraining the use of credentials: information flow policies to constrain propagation, and caveats to establish prerequisites and constrain the types of data covered by the credential.

As a more in-depth example of using such credentials, suppose Alice hosts a file sharing service. For a simpler presentation, we use free variables to refer to these files; for instance, $x_{1} : (k_{1} \text{ says } ph)$ is a variable that stores a photo (type $ph$) protected by $k_{1}$. For each such variable $x_{1}$, Alice has a credential $k_{1}^{-} \xrightarrow{pc} k_{1}^{-}$, and can give access to users by providing this credential or deriving a more restricted one. To access $x_{1}$, Bob does not need the full authority of Alice or $k_{1}$—a more restricted credential suffices:

$$\lambda(c : k_{1} \xrightarrow{Bob^{-}} k_{1}^{-} \land k_{1}^{-} ph)(Bob^{-})$$

$$bind \ x_{1} = c \ x_{1} \times (\forall k_{1} \in (\eta_{Bob^{-}} \land k_{1}^{-} x_{1}'))$$

Here, $c$ is a credential $k_{1} \xrightarrow{Bob^{-}} k_{1}^{-}$ whose polymorphic type has been instantiated with the photo type $ph$. This credential accepts a photo protected at $k_{1}$ and returns a photo protected at $k_{1}^{-} \land k_{1}^{-}$, which Bob is permitted to access.

The advantage of bearer credentials is that access to $x_{1}$ can be provided to principals other than $k_{1}$ in a decentralized way, without changing the policy on $x_{1}$. For instance, suppose Alice wants to issue a credential to Bob to access resources protected by $k_{1}$. Alice has a credential with type $k_{1}^{-} \xrightarrow{pc} k_{1}^{-}$, but she wants to ensure that only Bob (or principals Bob trusts) can use it. In other words, she wants to create a credential of type $k_{1} \xrightarrow{Bob^{-}} k_{1}^{-}$, which needs Bob’s integrity to use.

Alice can create such a credential using a wrapper that derives a more constrained credential from her original one.

$$\lambda(c : k_{1}^{-} \xrightarrow{pc} k_{1}^{-})(Alice^{-})$$

$$\Lambda X. \lambda(y; k_{1} \text{ says } X)(Bob^{-})$$

$$bind \ y' = y \times (\exists X \ (\eta_{k^{-}} y'))$$

Then Bob can use this credential to access $x_{1}$ by deriving a
credential of type \( k_1 \xrightarrow{\text{Bob}} \text{Bob} \rightarrow k_1^- \) ph using the function
\[
\lambda(c:k_1 \xrightarrow{\text{Bob}} k_1^-)[\text{Bob}]^+.
\]
\[
\lambda(y:k_1 \text{ says ph})[\text{Bob}]^+.
\]
\[
\text{bind } y' = c \text{ ph } y \text{ in } (\eta_{\text{Bob}^- \land k_1^-} y')
\]
which can be applied to obtain a value readable by Bob.

Bob can also use this credential to share photos with friends.

For instance, the function
\[
\lambda(c:k_1 \xrightarrow{\text{Bob}} k_1^-)[\text{Bob}]^+.
\]
\[
\text{assume } (\text{Carol}^- \Rightarrow \text{Bob}^-) \text{ in } \\
\lambda_{(-: \text{unit})}[\text{Carol}]^+.
\]
\[
\text{bind } x'_1 = c \text{ ph } x_1 \text{ in } (\eta_{\text{Carol}^- \land k_1^-} x'_1)
\]
creates a wrapper around a specific photo \( x_1 \). Only principals trusted by Carol may invoke the wrapper, which produces a value of type Carol^- \land k_1^- says ph, permitting Carol to access the photo.

The properties of FLAC let us prove many general properties about such bearer-credential programs; here, we examine three properties. For \( i \in \{1..n\} \), let
\[
\Gamma_{bc} = x_i : k_i \text{ says } s_i, c_i : \text{Alice says } (k_i^- \xrightarrow{\text{Bob}} k_i^-)
\]
where \( k_i \) is a primitive principal protecting the \( i \)th resource of type \( s_i \), and \( c_i \) is a credential for the \( i \)th resource and protected by Alice. Assume \( k_i \not\in \{\{\text{Alice, Friends, p}\} \text{ for all } i \text{ where p represents a (potentially malicious) user of Alice’s service, and Friends is a principal for Alice’s friends, (e.g., Friends } = (\text{Bob } \lor \text{Carol})\). Also, define \( pc_p = p^- \) and \( pc_A = \text{Alice}^- \).

- \( p \text{ cannot access resources without a credential.} \)
  For any \( e, \ell, \) and \( s' \) such that \( \Gamma_{bc} : pc_p \vdash e : \ell \cap p^- \text{ says } s' \), the value of \( e \) is independent of \( x_i \) for all \( i \).

- \( p \text{ cannot use unrelated credentials to access resources.} \)
  For any \( e, \ell, \) and \( s' \) such that
  \[
  \Gamma_{bc}, c_p : (k_i^- \xrightarrow{\text{Bob}} k_i^-) ; pc_p \vdash e : \ell \cap p^- \text{ says } s'
  \]
  the value \( e \) computes independent of \( x_i \) for \( i \neq 1 \).

- \( \text{Alice cannot disclose secrets by issuing credentials.} \)
  For all \( i \) and \( j \neq 1 \), define
  \[
  \Gamma'_b = x_i : k_i \text{ says } s_i, c_i : \text{Alice says } (k_i^- \xrightarrow{\text{Bob}} k_i^-),
  c_p : \text{Friends says } (k_j^- \xrightarrow{\text{Bob}} k_j^-)
  \]

  Then if \( \Gamma_{bc} : pc_A \vdash e : \ell \cap p^- \text{ says } (k_j^- \xrightarrow{\text{Bob}} k_j^-) \) for some \( e, \ell, \) and \( s' \), the value of \( e \) is independent of \( x_1 \).

These properties demonstrate the power of FLAC’s type system.

Section II-B. It implies that credentials issued by Alice do not leak information, in this case about Alice’s friends. By implementing bearer credentials in FLAC, we can demonstrate these three properties with relatively little effort.

VI. FLAC Proof theory

A. Properties of says

FLAC’s type system constrains how principals apply existing facts to derive new facts. For instance, a property of says in other authorization logics (e.g., Lampson et al. [1] and Abadi [2]) is that implications that hold for top-level propositions also hold for propositions of any principal \( \ell \):
\[
\vdash (s_1 \rightarrow s_2) \rightarrow (\ell \text{ says } s_1 \rightarrow \ell \text{ says } s_2)
\]
The \( pc \) annotations on FLAC function types refine this property. Each implication (in other words, each function) in FLAC is annotated with an upper bound on the information flow context it may be invoked within. To lift such an implication to operate on propositions protected at label \( \ell \), the label \( \ell \) must flow to the \( pc \) of the implication. Thus, for all \( \ell \) and \( s_i \),
\[
\vdash (s_1 \xrightarrow{pc[p]} s_2) \xrightarrow{pc} (\ell \text{ says } s_1 \xrightarrow{pc} \ell \text{ says } s_2)
\]
This judgment is a FLAC typing judgment in logical form, where terms have been omitted. We write such judgments with an empty typing context (as above) when the judgment is valid for any \( \Pi, \Gamma, \) and \( pc \). A judgment in logical form is valid if a proof term exists for the specified type, proving the type is inhabited. The above type has proof term
\[
\lambda(f : (s_1 \xrightarrow{pc[p]} s_2))[pc].
\]
\[
\lambda(x : \ell \text{ says } s_1)[pc]. \text{bind } x' = x \text{ in } (\eta_{\ell} x')
\]
In order to apply \( f \), we must first bind \( x \), so according to rules BindM and App, the function \( f \) must have a label at least as restrictive as \( pc \sqcup \ell \). All theorems of DCC can be obtained by encoding them as FLAC implications with \( pc = \top \rightarrow \), the highest bound. Since any principal \( \ell \) flows to \( \top \rightarrow \), such implications may be applied in any context.

These refinements of DCC’s theorems are crucial for supporting applications like commitment schemes and bearer credentials. Recall from Sections V-A and V-B that the security of these mechanisms relied in part on restricting the \( pc \) to a specific principal’s integrity. Without such refinements, principal \( q \) could open principal \( p \)’s commitments using open, or create credentials with \( p \) authority: \( p^- \xrightarrow{pc} p^- \).

Other properties of \( says \) common to DCC and other logics (cf. [27] for examples) are similarly refined by \( pc \) bounds. Two examples are:
\[
\vdash s \xrightarrow{pc} \ell \text{ says } s \text{ which has proof term: } \\
\lambda(x : s)[pc] \cdot (\eta_{\ell} x)
\]
\[
\vdash \ell \text{ says } (s_1 \xrightarrow{pc[p]} s_2) \xrightarrow{pc} (\ell \text{ says } s_1 \xrightarrow{pc} \ell \text{ says } s_2)
\]
with proof term:
\[
\lambda(f : \ell \text{ says } (s_1 \xrightarrow{pc[p]} s_2))[pc]. \text{bind } x' = x \text{ in } \\
\lambda(y : \ell \text{ says } s_1)[pc]. \text{bind } y' = y \text{ in } (\eta_{x'} x')
\]
As in DCC, chains of says are commutative in FLAC:

\[ \vdash \ell_1 \text{ says } \ell_2 \text{ says } s \Rightarrow \ell_2 \text{ says } \ell_1 \text{ says } s \]

with proof term

\[ \lambda(x: \ell_1 \text{ says } \ell_2 \text{ says } s)[pc]. \]

\[ \text{bind } y = x \text{ in bind } z = y \in (\eta_{\ell_2} (\eta_{\ell_1} z)) \]

In some logics with different interpretations of says (e.g., CCD [28]) differently ordered chains are distinct, but here we find commutativity appealing since it matches the intuition from information flow control. When principal \( \ell_1 \) says that \( \ell_2 \) says \( s \), we should protect \( s \) with a policy at least as restrictive as both \( \ell_1 \) and \( \ell_2 \), i.e., the principal \( \ell_1 \sqcup \ell_2 \). Since \( \sqcup \) is commutative, who said what first is irrelevant.

B. Dynamic Hand-off

Many authorization logics support delegation using a “hand-off” axiom. In DCC, this axiom is actually a provable theorem:

\[ \vdash (q \text{ says } (p \Rightarrow q)) \Rightarrow (p \Rightarrow q) \]

where \( p \Rightarrow q \) is shorthand for

\[ \forall X. (p \text{ says } X \Rightarrow q \text{ says } X) \]

However, \( p \Rightarrow q \) is only inhabited if \( p \subseteq q \) in the security lattice. Thus, DCC can reason about the consequences of \( p \subseteq q \) (whether it is true for the lattice or not), but a DCC program cannot produce a term of type \( p \Rightarrow q \) unless \( p \subseteq q \).

FLAC programs, on the other hand, can create new trust relationships from delegation expressions using assume terms. The type analogous to \( p \Rightarrow q \) in FLAC is

\[ \forall X. (p \text{ says } X \Rightarrow q \text{ says } X) \]

which we wrote as \( p \Rightarrow q \) in Section V-B. FLAC programs construct terms of this type from proofs of authority, represented by terms with acts-for types. This feature enables a more general form of hand-off, which we state formally below.

Proposition 1 (Dynamic hand-off). For all \( \ell \) and \( pc' \), let \( pc = \ell \Rightarrow \nabla (p^-) \land q^- \)

\[ (\nabla (q^-) \Rightarrow \nabla (p^-)) \Rightarrow (p \subseteq q) \Rightarrow \]

\[ \forall X. (p \text{ says } X \Rightarrow pc' \Rightarrow q \text{ says } X) \]

Proof term.

\[ \lambda(pf_1:(\nabla(q^-) \Rightarrow \nabla(p^-)))[pc]. \]

\[ \lambda(pf_2:(p \subseteq q))[pc]. \]

\[ \text{assume } pf_1 \text{ in assume } pf_2 \text{ in } \]

\[ \Lambda X. \lambda(x: p \text{ says } X)[pc']. \text{ bind } x' = x \in (\eta_q x') \]

The principal \( pc = \ell \Rightarrow \nabla (p^-) \land q^- \) restricts delegation (hand-off) to contexts with the integrity of \( \nabla (p^-) \land q^- \). The two arguments are proofs of authority with acts-for types: a proof of \( \nabla (q^-) \Rightarrow \nabla (p^-) \) and a proof of \( p \subseteq q \). The \( pc \) ensures that the proofs have sufficient integrity to be used in assume terms since it has the integrity of both \( \nabla (p^-) \) and \( q^- \). Note that low-integrity or confidential delegation values must first be bound via \text{bind} \ before the above term may be applied. Thus the \( pc \) would reflect the protection level of both arguments. Principals \( \ell \Rightarrow p \) and \( pc' \) are unconstrained.

Dynamic hand-off terms give FLAC programs a level of expressiveness and security not offered by other authorization logics. Observe that \( pc' \) may be chosen independently of the other principals. This means that although the \( pc \) prevents low-integrity principals from creating hand-off terms, a high-integrity principal may create a hand-off term and provide it to an arbitrary principal. Hand-off terms in FLAC, then, are similar to capabilities since even untrusted principals may use them to change the protection level of values. Unlike in most capability systems, however, the propagation of hand-off terms can be constrained using information flow policies.

Terms that have types of the form in Proposition 1 illustrate a subtlety of enforcing information flow in an authorization mechanism. Because these terms relabel information from one protection level to another protection level, the transformed information implicitly depends on the proofs of authorization. FLAC ensures that the information security of these proofs is protected—like that of all other values—even as the policies of other information are being modified. Hence, authorization proofs cannot be used as a side channel to leak information.

VII. SEMANTIC SECURITY PROPERTIES OF FLAC

A. Delegation invariance

FLAC programs dynamically extend trust relationships, enabling new flows of information. Nevertheless, well-typed programs have end-to-end semantic properties that enforce strong information security. These properties derive primarily from FLAC’s control of the delegation context. The \text{ASSUME} rule ensures that only high-integrity proofs of authorization can extend the delegation context, and furthermore that such extensions occur only in high-integrity contexts.

That low-integrity contexts cannot extend the delegation context turns out to be a crucial property. This property allows us to state a useful invariant about the evaluation of FLAC programs. Recall that \text{assume} terms evaluate to \text{where} terms in the FLAC semantics. Thus, FLAC programs typically compute values containing a hierarchy of nested \text{where} terms. The terms record the values whose types were used to extend the delegation context during type checking.

For a well-typed FLAC program, we can prove that certain trust relationships could not have been added by the program. Characterizing these relationships requires a concept of the minimal authority required to cause one principal to act for another. Although similar, this idea is distinct from the voice of a principal. Consider the relationship between \( a \) and \( a \land b \). The voice of \( a \land b \), \( \nabla (a \land b) \), is sufficient integrity to add a delegation \( a \land b \) to \( a \) so that \( a \Rightarrow a \land b \). Alternatively, having only the integrity of \( \nabla (b) \) is sufficient to add a delegation \( a \Rightarrow b \), which also results in \( a \Rightarrow a \land b \). To precisely characterize which trust relationships can not be added by program, we need to identify this minimal integrity \( \nabla (b) \) given the pair of
principals $a$ and $a \land b$. The following definitions are in service of this goal.

The first definition formalizes the idea that two principals are considered equivalent in a given context if they act for each other.

**Definition 1 (Principal Equivalence).** We say that two principals $p$ and $q$ are equivalent in $\Pi; pc$, denoted $\Pi; pc \vdash p \equiv q$, if

$$H; c; pc; \ell \vdash p \equiv q \text{ and } H; c; pc; \ell \vdash q \equiv p.$$ 

Next, we define the factorization of two principals in a given context. For two principals, $p$ and $q$, their factorization involves representing $q$ as the conjunction of two principals $q_s \land q_d$ such that $p \gg q_s$ in the desired context. Note that $p$ need not act for $q_d$.

**Definition 2 (Factorization).** A $(\Pi; pc)$-factorization of an ordered pair of principals $(p, q)$ is a tuple $(p, q_s, q_d)$ such that $\Pi; pc \vdash q \equiv q_s \land q_d$ and $H; c; pc; \ell \vdash p \equiv q$.

A factorization is static if $\Pi = \emptyset$ (and thus $L \vdash p \gg q_s$).

Finally, the minimal factorization of $p$ and $q$ is a $q_s$ and $q_d$ such that $q_s$ has greater authority and $q_d$ has less authority than any other factorization of $p$ and $q$ in the same context.

**Definition 3 (Minimal Factorization).** A $(\Pi; pc)$-factorization $(p, q_s, q_d)$ of $(p, q)$ is minimal if for any $(\Pi; pc)$-factorization $(p, q_s', q_d)$ of $(p, q)$,

$$H; c; pc; \ell \vdash q_s \gg q_s' \text{ and } H; c; pc; \ell \vdash q_d \gg q_d$$

The minimal factorization $(p, q_s, q_d)$ of $p$ and $q$ is well-typed and it is sufficient authority to cause $p$ to act for $q$. Because $q_s$ is the principal with the greatest authority such that $p \gg q_s$ and $q \equiv q_s \land q_d$, then speaking for $q_d$ is sufficient authority to cause $p$ to act for $q$ since adding the delegation $p \gg q_d$ would imply that $p \gg q$. This intuition also matches with the fact that $H; c; pc; \ell \vdash p \gg q_d$ if and only if $q_d = \bot$, which is the case if and only if $H; c; pc; \ell \vdash p \gg q$. Observe also that minimal $(\Pi; pc)$-factorizations are also trivially unique up to equivalence.

Since the $q_d$ component of minimal factorization can be thought of as the “gap” in authority between two principals, we use $q_d$ to define the notion of principal subtraction.

**Definition 4 (Principal Subtraction).** Let $(p, q_s, q_d)$ be the minimal $(\Pi; pc)$-factorization of $(p, q)$. We define $q - p$ in $\Pi; pc$ to be $q_d$. That is, $\Pi; pc; pc \not\vdash q - p \equiv q_d$. Note that $q - p$ is not defined outside of a judgement context.

Lemma 1 proves that minimal factorizations exist for all contexts and principals, so principal subtract is well defined.

**Lemma 1 (Minimal Factorizations Exist).** For any context $(\Pi; pc)$ and principals $p, q$, there exists a minimal $(\Pi; pc)$-factorization of $(p, q)$.

**Proof.** Given $(p, q)$, we first let $q_s = q \lor q$. By definition, $H; c; pc; \ell \vdash p \equiv q \lor q$, and for all factorizations $(p, q_s', q_d)$,

$$H; c; pc; \ell \vdash p \gg q_s' \text{ and } H; c; pc; \ell \vdash q \gg q_s', \text{ so } H; c; pc; \ell \vdash q \gg q_s'.$$

Now let $D = \{ r \in L \mid \Pi; pc \vdash q \equiv q_s \land r \}$. All principals in $L$ can be represented as a finite set of meets and joins of names in $N$ so $q$ and $q_s$ are finite. $\Pi$ is also finite, adding only finitely-many dynamic equivalences, so $D$ is finite up to equivalence. Moreover, $q \in D$ trivially, so $D$ is non-empty and thus we can define $q_d = \bigvee D$.

Now let $(p, q_s, q_d)$ be any factorization of $(p, q)$. We must show that $H; c; pc; \ell \vdash q_d \gg q_d$. First we see that $\Pi; pc; pc \not\vdash q \equiv q_s \land q_d$. $H; c; pc; \ell \vdash q \gg q_s$ gives us $H; c; pc; \ell \vdash q \gg q_s \land q_d \gg q$ and the definitions of $q_s$ and $q_d$ as parts of a factorization of $(p, q)$ give us the other direction.

Therefore, by construction, $q_d \in D$, so by the definition of $\lor$ and $q_d$, $H; c; pc; \ell \vdash q_d \gg q_d$. Thus we see that $(p, q_s, q_d)$ is a minimal $\Pi; pc$-factorization of $(p, q)$.

We can now state precisely which trust relationships may change in a given information flow context.

**Lemma 2 (Delegation Invariance).** Let $\Pi; \Gamma; pc \vdash e : s$ such that $e \rightarrow e'$ where $v$. Then there exist $r, t \in L$ and $\Pi' = \Pi; (r^s \gg t^s) \mid pc$ such that $\Pi; \Gamma; pc \vdash v : (r^s \gg t^s)$ and $\Pi'; \Gamma; pc \vdash e' : s$. Moreover, for all principals $p$ and $q$ if $H; c; pc; e \neq p \not\vdash \Delta (\pi^q) - \Delta (\pi^p)$, then

$$\Pi'; pc; pc \not\vdash \pi^s \gg \pi^q.$$ 

**Proof.** See Appendix A. 

First, Lemma 2 says that at each step of evaluation, there exists a $\Pi'$ such that $e'$ is well typed. More importantly, this $\Pi'$ has a useful invariant. If $pc$ does not speak for the authority required to cause $q$ to delegate to $p^s$, then $\Pi$ and $\Pi'$ must agree on the trust relationship of $p^s$ and $q^s$.

**B. Noninterference**

**Lemma 2** is critical for our proof of noninterference, a result that states that public and trusted output of a program cannot depend on restricted (secret or untrustworthy) information. Our proof of noninterference for FLAC programs relies on a proof of subject reduction under a bracketed semantics, based on the proof technique of Pottier and Simonet [20]. This technique is relatively standard, so we omit it here. The complete proof of subject reduction is in our technical report [29]; proofs for other results are found in Appendix A.

In other noninterference results based on bracketed semantics, including [20], noninterference follows almost directly from the proof of subject reduction. This is because the subject reduction proof shows that evaluating a term cannot change its type. In FLAC, however, subject reduction alone is insufficient; evaluation may enable flows from secret or untrusted inputs to public and trusted types.

To see how, suppose $e$ is a well-typed program according to $\Pi; \Gamma; x : s; pc \vdash e : s'$. Furthermore, let $H$ be a principal such that $\Pi; pc \vdash H \leq s$ and $\Pi; pc \not\vdash H \leq s'$. In other words, $x$ is a “high” variable (more restrictive; secret and untrusted), and $e$ evaluates to a “low” result (less restrictive;
public and trusted). In [20], executions that differ only in secret or untrusted inputs must evaluate to the same value, since otherwise the value would not be well typed. In FLAC, however, if the pc has sufficient integrity, then an assume term could cause \( \Pi' \vdash pc \vdash H \leq s' \) to hold in a delegation context \( \Pi' \) of a subterm of \( e \). The key to proving our result relies on using Lemma 2 to constrain the assumptions that can be added to \( \Pi' \). Thus noninterference in FLAC is dependent on \( H \) and its relationship to \( pc \) and the type \( s' \).

For more precision, Theorem 1 describes noninterference on confidentiality and integrity separately. It states that for some principal \( H^+ \) that flows to \( s \) but not \( \ell \) says bool, if \( pc \) cannot cause \( H^\rightarrow \) to speak for \( \nabla(H^\rightarrow) \) for confidentiality, or \( \ell^\rightarrow \) for integrity, then an execution of \( e \) that differs only in the value of \( s \)-typed inputs, the computed values must be equal.\(^{15}\)

**Theorem 1** (Noninterference). Let \( \Pi; \Gamma; x : s; pc \vdash e : \ell \) says bool. If there exists some \( H \) and \( \pi \) such that

\[
1) \ \Pi; \Gamma; x : s; pc \vdash H^\pi \leq s \\
2) \ H; c; pc; \ell \not\vdash H^\pi \subseteq \ell^\pi \\
3a) if \( \pi = \rightarrow \) then \( H; c; pc; \ell \not\vdash pc \vdash \nabla(H^\rightarrow) - H^\rightarrow \) \\
3b) if \( \pi = \leftarrow \) then \( H; c; pc; \ell \not\vdash pc \vdash (\ell - H)^\rightarrow \)
\]

then for all \( v_1, v_2 \) with \( \Pi; \Gamma; pc \vdash v_i : s \), if \( e[x \mapsto v_i] \rightarrow^* v'_i \), then \( v'_1 = v'_2 \).

**Proof.** By Lemma 2 and subject reduction on a bracketed semantics. See Appendix A for details.

Condition 1 identifies \( s \) as a “high” type—at least as restricted as \( H \). Condition 2 identifies \( \ell \) says bool as a “low” type, to which information labeled \( H \) should not flow. Conditions 3a and 3b identify \( pc \) as having integrity compared to the difference between \( H^\rightarrow \) and the voice \( H^\rightarrow \) or \( \ell^\rightarrow \). Given these conditions, if \( e \) evaluates to \( v'_1 \) when \( x = v_1 \) and \( v'_2 \) when \( x = v_2 \), then \( v'_1 = v'_2 \).

Noninterference is a key tool for obtaining many of the security properties we seek. For instance, noninterference is essential for verifying the properties of commitment schemes discussed in Section V-A. The proofs of these properties are described in Appendix B.

C. Robust declassification

Using our noninterference result, we obtain a more general semantic security property for FLAC programs. That property, robust declassification [31], requires disclosures of secret information to be independent of low-integrity information. Robust declassification permits some confidential information to be disclosed to an attacker, but attackers can influence neither the decision to disclose information nor the choice of what information is disclosed. Therefore, robust declassification is a more appropriate security condition than noninterference when programs are intended to disclose information.

15It is standard for noninterference proofs in languages with higher-order functions to restrict their results to non-function types (cf. [20], [11], [30]). In this paper, we prove noninterference for boolean types, encoded as bool = (unit + unit). With an appropriate equivalence relation on terms, this noninterference result can be lifted to more general types.

Programs and contexts that meet the requirements of Theorem 1 trivially satisfy robust declassification since no information is disclosed. In higher-integrity contexts where the pc speaks for \( H^\rightarrow \) (and thus may influence its trust relationships), FLAC programs exhibit robust declassification.

Following Myers et al. [32], we extend our set of terms with a “hole” term \([\bullet]\) representing portions of a program that are under the control of an attacker. We extend the type system with the following rule for holes with lambda-free types:

\[
[\text{HOLE}] \quad \Pi; pc \vdash H^\rightarrow \leq t \\
\Pi; pc; pc \vdash H^\rightarrow \nabla(pc) \\
\Pi; \Gamma; pc \vdash [\bullet] : t
\]

We write \( e[\bullet] \) to denote a program \( e \) with holes. Let an attack be a vector \( \vec{a} \) of terms and \( e[\vec{a}] \) be the program where \( a_i \) is substituted for \( \bullet \). An attack \( \vec{a} \) is a fair attack [31] on a well-typed program with holes \( e[\bullet] \) if the program \( e[\vec{a}] \) is also well typed. Unfair attacks give the attacker enough power to break security directly, without exploiting existing declassifications. Fair attacks represent the power of the attacker over low-integrity portions of the program.

**Theorem 2** (Robust declassification). Let \( e[\bullet] \) be a program such that

\[
1) \ \Pi; \Gamma; x : s; pc \vdash e[\bullet] : \ell \) says bool \\
2) \ H; c; pc; \ell \not\vdash pc \vdash (\ell - h)^\rightarrow \\
\]

Then for all attacks \( \vec{a}_1 \) and \( \vec{a}_2 \) and all inputs \( v \) such that

\[
\Pi; \Gamma; x : s; \vec{a}_1; pc \vdash e[\vec{a}_1][x \mapsto v] \rightarrow^* v'_1 \\
\Pi; \Gamma; pc \vdash v : s, if \ e[\vec{a}_1][x \mapsto v] \rightarrow^* v'_1, then \ v'_1 = v'_2.
\]

**Proof.** By Lemma 2 and a generalization of Theorem 1 under attacks. See Appendix A for details.

Our formulation of robust declassification is in some sense more general than previous definitions since it permits some endorsements, albeit restricted to untrusted principals that cannot influence the trust relationships of \( \ell^\rightarrow \), the integrity of the result. Previous definitions of robust declassification [32], [31] forbid endorsement altogether; qualified robustness [32] permits endorsement but offers only probabilistic security.

VIII. RELATED WORK

Many languages and systems for authorization or access control have combined aspects of information security and authorization (e.g., [33], [34], [35], [8], [36], [9]) in dynamic settings. However, almost all are susceptible to security vulnerabilities that arise from the interaction of information flow and authorization [12]: probing attacks, delegation loopholes, poaching attacks, and authorization side channels.

DCC [11], [2] has been used to model both authorization and information flow, but not simultaneously. DCC programs are type-checked with respect to a static security lattice, whereas FLAC programs can introduce new trust relationships during evaluation, enabling more general applications.

Boudol [37] defines terms that enable or disable flows for a lexical scope, similar to assume terms, but does not restrict their usage. Rx [8] and RTI [9] use labeled roles to represent
information flow policies. The integrity of a role restricts who may change policies. However, information flow in these languages is not robust [32]: attackers may indirectly affect how flows change when authorized principals modify policies.

Some prior approaches have sought to reason about the information security of authorization mechanisms. Becker [38] discusses probing attacks that leak confidential information to an attacker. Garg and Pfennig [39] present a logic that ensures assertions made by untrusted principals cannot influence the truth of statements made by other principals.

Previous work has studied information flow control with higher-order functions and side effects. In the SLam calculus [40], implicit flows due to side effects are controlled via indirect reader annotations on types. Zdancewic and Myers [41] and Flow Caml [20] control implicit flows via pc annotations on function types. FLAC also controls side effects via a pc annotation, but here the side effects are changes in trust relationships that define which flows are permitted. Tse and Zdancewic [22] also extend DCC with a program-counter label but for a different purpose: their pc tracks information about the protection context, permitting more terms to be typed.

DKAL* [42] is an executable specification language for authorization protocols, simplifying analysis of protocol implementations. FLAC may be used as a specification language, but FLAC offers stronger guarantees regarding the information security of specified protocols. Errors in DKAL* specifications could lead to vulnerabilities. For instance, DKAL* provides no intrinsic guarantees about confidentiality, which could lead to authorization side channels or probing attacks.

The Jif programming language [21], [43] supports dynamically computed labels through a simple dependent type system. Jif also supports dynamically changing trust relationships through operations on principal objects [44]. Because the signatures of principal operations (e.g., to add a new trust relationship) are missing the constraints imposed by FLAC, authorization can be used as a covert channel. FLAC shows how to close these channels in languages like Jif.

Dependently-typed languages are often expressive enough to encode authorization policies, information flow policies, or both. The F* [45] type system is capable of enforcing information flow and authorization policies. Typing rules like those in FLAC could probably be encoded within its type system, but so could incorrect, insecure rules. Thus, FLAC contributes a model for encodings that enforce strong information security. Aura [46] embeds a DCC-based proof language and type system in a dependently-typed general-purpose functional language. As in DCC, Aura programs may derive new authorization proofs using existing proof terms and a monadic bind operator. However, since Aura only tracks dependencies between proofs, it is ill-suited for reasoning about the end-to-end information-flow properties of authorization mechanisms.

IX. CONCLUSION

Existing security models do not account fully for the interactions between authorization and information flow. The result is that both the implementations and the uses of authorization mechanisms can lead to insecure information flows that violate confidentiality or integrity. The security of information flow mechanisms can also be compromised by dynamic changes in trust. This paper has proposed FLAC, a core programming language that coherently integrates these two security paradigms, controlling the interactions between dynamic authorization and secure information flow. FLAC offers strong guarantees and can serve as the foundation for building software that implements and uses authorization securely. Further, FLAC can be used to reason compositionally about secure authorization and secure information flow, guiding the design and implementation of future security mechanisms.

ACKNOWLEDGMENTS

We thank Mike George, Elaine Shi, and Fred Schneider for helpful discussions, our anonymous reviewers for their comments and suggestions, and Jed Liu and Matt Stillerman for feedback on early drafts. Ethan Cецehetti discovered several technical errors in our original formalization, and was instrumental in addressing them for this corrected version. This work was supported by grant N00014-13-1-0089 from the Office of Naval Research, by MURI grant FA9550-12-1-0400, and by a grant from the National Science Foundation (CCF-0964409). This paper does not necessarily reflect the views of any of these sponsors.

REFERENCES

Syntax extensions

\[ v \ ::= \ldots \mid \{v \}\ ]

Typing extensions

\[ \Pi; \Gamma; \text{pc} \vdash e_1 : s \quad \Pi; \Gamma; \text{pc} \vdash e_2 : s \]

Evaluation extensions

\[ e_1 \rightarrow e'_1 \quad e_1 = e'_1 \quad \{i, j\} = \{1, 2\} \]

\[ \Pi; \text{pc} \vdash (H \cup \text{pc})^n \subseteq \text{pc}^n \]

\[ \Pi; \text{pc} \vdash H^n \leq s \]

\[ \Pi; \text{pc} \vdash \{e_1 \} \vdash s \]

\[ \Pi; \text{pc} \vdash \{e_1 \} \vdash s \]

\[ \Pi; \text{pc} \vdash \{e_1 \} \vdash s \]

\[ \Pi; \text{pc} \vdash \{e_1 \} \vdash s \]

Fig. 10: Extensions for bracketed semantics

APPENDIX A

PROOFS OF NONINTERFERENCE AND ROBUSTNESS

Lemma 3 (Soundness). If \( e \rightarrow^\ast e' \) then \( |e|_1 \rightarrow |e'|_1 \) and \( |e|_2 \rightarrow |e'|_2 \).
Proof. By inspection of the rules in Figure 4 and Figure 10.

Lemma 4 (Completeness). If \([e]_1 \rightarrow^{\ast} v_1 \text{ and } [e]_2 \rightarrow^{\ast} v_2\), then there exists some \(v\) such that \(e \rightarrow^{\ast} v\).

Proof. Assume \([e]_1 \rightarrow^{\ast} v_1 \text{ and } [e]_2 \rightarrow^{\ast} v_2\). The extended set of rules in Figure 10 always move brackets out of subterms, and therefore can only be applied a finite number of times. Therefore, by Lemma 3, if \(e\) diverges, either \([e]_1\) or \([e]_2\) diverge; this contradicts our assumption. It remains to be shown that if the evaluation of \(e\) gets stuck, either \([e]_1\) or \([e]_2\) gets stuck. This is easily proven by induction on the structure of \(e\). Therefore, since we assumed \([e]_1 \rightarrow^{\ast} v_1\), then \(e\) must terminate. Thus, there exists some \(v\) such that \(e \rightarrow^{\ast} v\).

Lemma 5 (Substitution). If \(\Pi; \Gamma, x : s ; pc \vdash e : s \text{ and } \Pi; \Gamma; pc \vdash v : s\) then \(\Pi; \Gamma; pc \vdash e[x \mapsto v] : s\).

Proof. By induction on the typing derivation for \(e\).

Lemma 6 (Values). If \(\Pi; \Gamma; pc \vdash v : s\), then \(\Pi; \Gamma; pc' \vdash v : s\) for any \(pc'\).

Proof. By induction on the derivation of \(\Pi; \Gamma; pc \vdash e : s\).

Lemma 7 (Robust transitivity). If \(\Pi; pc; \ell \vdash p \geq q \text{ and } \Pi; pc; \ell \vdash q \geq r\), then \(\Pi; pc; \ell \vdash p \geq r\).

Proof. This is a consequence of the FLAM's Principal Factorization Lemma [12]. See [47] for Coq proof.

Lemma 8 (Voices). If \(\Pi; pc; \ell \vdash q \text{ then } \Pi; pc; \ell \vdash \\nabla(p) \geq \nabla(q)\).

Proof. By induction on the derivation of \(\Pi; pc; \ell \vdash q\). Let \(\Pi; pc; \ell \vdash q\) implies \(\Pi; pc; \ell \vdash \nabla(q)\) (verified in [47]), and each \((p \geq q | \ell) \in \Pi\) has \(\Pi; pc; \ell \vdash \nabla(p) \geq \nabla(q)\), so \((p \geq q | \ell) \in \Pi\) implies \(\Pi; pc; \ell \vdash \nabla(p) \geq \nabla(q)\). The remaining cases are trivial.

Lemma 9 (pc reduction). If \(\Pi; pc; pc' \vdash e : s \text{ and } \Pi; pc; pc' \vdash pc \subseteq pc'\), then \(\Pi; pc; \vdash [e]_1 : s\).

Proof. By induction on the derivation of \(\Pi; pc; pc' \vdash e : s\) and Lemma 7. Note that BRACKET does not preserve this property, hence the projection of \(e\) is necessary.

Theorem 3 (Subject reduction). Suppose \(\Pi; pc \vdash e : s \text{ and } [e]_i \rightarrow [e']_i\). If \(i \in \{1, 2\}\) then assume \(\Pi; pc; pc \vdash H \subseteq pc\). Then \(\Pi; pc; \vdash e' : s\).

Proof. By induction on the derivation of \([e]_1 \rightarrow [e']_1\). See the technical report [29] for details.

We extend the FLAM principal factorization lemma [12] to minimal factorizations.

Lemma 10 (Delegation Factorization). If \(\Pi; pc; \ell \vdash p \geq q\) and \((p, q, s)\) is the minimal static factorization of \(p, q\), then \(\Pi; pc; \ell \vdash pc \geq \nabla(q)\).

Proof. A Coq-verified proof in [47] showed that there is some static factorization \((p, q', s')\) such that \(\Pi; pc; pc \vdash \ell \vdash p \geq q'\) and \(\Pi; pc; pc \vdash \ell \vdash pc \geq \nabla(qd)\). By the definition of minimal factorization, \(L \vdash qd \geq qd\), so \(L \vdash \nabla(qd) \geq \nabla(qd)\), and by transitivity on static acts-for-relationships, \(\Pi; pc; pc \vdash \ell \vdash p \geq qd\) and \(\Pi; pc; pc \vdash pc \geq \nabla(qd)\).

Lemma 2 (Delegation Invariance). Let \(\Pi; \Gamma; pc \vdash e : s \text{ such that } e \rightarrow e' \text{ where } v.\) Then there exist \(t, t' \in L\) and \(\Pi' = L \vdash q \rightarrow t\) and \(\Pi' ; \Gamma ; \beta; pc \vdash e' : s.\) Moreover, for all principals \(p \text{ and } q\) if \(\Pi; pc; pc \vdash pc \geq \nabla(q) - \nabla(p)\), then \(\Pi' ; pc ; pc \vdash pc \geq q\).

Proof. Let \((p, q, s)\) be the minimal \((\Pi; pc)\)-factorization of \((p, q)\). First we note that \(qd \neq \perp\) and thus \(\Pi; pc; pc \vdash pc \geq qd\). Now assume for contradiction that \(\Pi' ; pc ; pc \vdash pc \geq q\).

We claim that \(\Pi ; pc ; pc \vdash pc \geq t' \geq qd\). Assume for contradiction that this is false. By transitivity \(\Pi' ; pc ; pc \vdash pc \geq qd\), and since \(\Pi ; pc ; pc \vdash pc \geq qd\), any derivation of this must use R-ASSUME with the deletion \((t' \geq t \vdash pc)\). This means that \(\Pi; pc; pc \vdash qd \equiv t' \geq qd\) for some \(q'\) where \(\Pi; pc; pc \vdash pc \geq qd\). Assume without loss of generality that \(\Pi; pc; pc \vdash p \geq qd\). Otherwise the same argument would give us that \(\Pi; pc; pc \vdash qd \equiv t' \geq qd\), so \(qd = t' \geq qd\) so we can let \(q' = qd\). Since all representations are finite and with each iteration we remove at least one term from \(qd\), we can only do this finitely many times until eventually \(\Pi; pc; pc \vdash pc \geq qd\) (possibly because \(qd = \perp\)). However, this means that \((p, q, s, qd)\) is a valid \((\Pi; pc)\)-factorization of \((p, q)\). Since \(\Pi; pc; pc \vdash pc \geq qd\), it is also the case that \(\Pi; pc; pc \vdash pc \geq t' \geq qd\), which contradicts the assumption that \((p, q, s)\) is minimal and thus \(\Pi; pc; pc \vdash pc \geq qd\).

\(\rightarrow\) If \(p \rightarrow\), then by WHERE with \(pc' = pc\), \(\Pi; pc; pc \vdash qd \equiv \nabla(t')\) and by Lemma 8, \(\Pi; pc; pc \vdash \nabla(t') \geq \nabla(qd)\). Thus, by transitivity, \(\Pi; pc; pc \vdash pc \geq \nabla(qd)\) which contradicts our assumption. Similarly, if \(\leftarrow\), by WHERE with \(pc' = pc\), \(\Pi; pc; pc \vdash pc \geq t'\), so by transitivity, \(\Pi; pc; pc \vdash pc \geq qd\) which again contradicts our assumption.

Theorem 1 (Noninterference). Let \(\Pi; \Gamma; x : s ; pc \vdash e : \ell \text{ says bool}\). If there exists some \(H\) and \(\pi\) such that

1) \(\Pi; pc \vdash H \leq s\)
2) \(\Pi; pc; pc \vdash \ell \vdash H \leq \ell'\)
3) \(a)\) if \(\pi = \rightarrow\) then \(\Pi; pc; pc \vdash H(\ell') - H + \beta\)
5) \(b)\) if \(\pi = \leftarrow\) then \(\Pi; pc; pc \vdash H(\ell) - H + \beta\)
then for all \(v_1, v_2\) with \(\Pi; pc \vdash v_1 : s\) if \(e[x \mapsto v_1] \rightarrow^{\ast} v'_1\), then \(v'_1 = v_2\).

Proof. To prove this, we employ the bracketed semantics. By Lemma 6 \(\Pi; \Gamma; \Gamma \vdash v_1 : s\) and thus, for any \(H, \Pi; \Gamma; pc \vdash (v_1 \mid v_2) : s\).

We now examine the term \(e[x \mapsto (v_1 \mid v_2)]\). By Lemma 5, \(\Pi; \Gamma; pc \vdash (v_1 \mid v_2) : \ell \text{ says bool}\), and by assumption
\[ e[x \rightarrow v_1] \rightarrow^* v_1. \] Thus by Lemma 4 there is some \( v' \) such that \( e[x \rightarrow (v_1 \mid v_2)H^\sharp] \rightarrow^* v' \) and, moreover, by Theorem 3 Π; Γ; pc \models \psi' : Π \models \psi \; \text{says} \; \text{bool}.

We will show that \( v'_1 = v'_2 \) by showing that \( v' \) does not contain a bracketed term. First we note that since \( H; c; pc; \ell \not\models H^\sharp \subseteq \ell^\approx \), \( v' \) cannot itself be a bracketed term. Similarly, it cannot be the case that \( v' = (\eta \; w) \) where \( w \) is bracketed. The only other option is that \( v' = w \) where \( w \) contains a bracketed term. We will prove this is not the case by induction on the number of where \( \psi \) clauses.

For the base case with zero clauses, we have already shown this. Now we assume that \( v' = w \) where \( u \) and \( w \) is not itself a where \( \psi \) clause containing a bracketed term. There are two cases to consider, depending on \( \pi \).

Case (\( \pi = \rightarrow \)). In this case condition 2 means \( H; c; pc; \ell \not\models \ell \rightarrow H^\approx \). Since \( H; c; pc; \ell \not\models pc \models \nabla(H^\approx) - H^\approx \), Lemma 2 gives us that there is some Π; Γ; pc \models u : Δ \models \psi \; \text{says} \; \text{bool} and Π; Γ; pc \models \ell \rightarrow H^\approx. \) Thus \( v' \) cannot itself be a bracketed term (or \((\eta \; w')\)), and by the inductive hypothesis it is not a where \( \psi \) clause containing a bracketed term, thus proving that \( v' \) contains no bracketed terms.

Case (\( \pi = \leftarrow \)). In this case condition 2 means \( H; c; pc; \ell \not\models H^\approx \subseteq \ell^\approx \). Since \( H; c; pc; \ell \not\models pc \models (\ell - H)^\approx \), Π; Γ; pc \models \psi \; \text{says} \; \text{bool} and the same argument as the previous case show that \( w \) contains no bracketed terms.

Thus we have that \( v' \) contains no bracketed terms, so \( v'_1 = [v'_1]_1 = [v'_2]_2 = v'_2 \).

To prove FLAC enforces robust declassification, we first prove a stronger property we call noninterference under attacks. This property demonstrates that attacks by low integrity principals cannot create interfering flows of information. This result uses the following property of principal subtraction.

**Lemma 11.** For all principals \( p, q, \) and \( r \),

\[ H; c; pc; \ell \models (p \land q) \land (q - r) \not\models p - r. \]

**Proof.** Let \( \Pi_d \) such that Π; Γ; pc \models Π_d \equiv (p - q) \land (q - r).

Now consider the following expression

\[ \Pi; pc; \ell \models [\Pi_d \lor p] \land (p \lor r) \equiv p \lor (\Pi_d \land p) \]

\[ \equiv p \lor [(p - q) \land (r - (q - r))] \]

\[ \equiv p \lor [(p - q) \land q] \]

\[ \equiv p \lor p \]

\[ \equiv p. \]

Thus we see that for any (\( \Pi; pc \))-factorization \((r, p \land r, p_d)\) of \((r, p); H; c; pc; \ell \models \Pi_d \lor p \not\models p_d\) which means \( H; c; pc; \ell \models \Pi_d \not\models p_d \). In particular, since \((p - r)\) represents the minimal such factorization, \( H; c; pc; \ell \models (p - q) \land (q - r) \not\models p - r. \)

**Lemma 12.** (Noninterference under attacks). Let \( e[\psi] \) be a program such that

1) \( \Pi; \pi; pc \models e[\psi] : \psi \models \text{bool} \)

2) For all \( (p \not\models q \mid pc') \in \Pi, H; c; pc; \ell \models pc' \subseteq pc \)

3) \( H; c; pc; \ell \not\models H^\approx \subseteq \ell^\approx \)

4a) if \( \pi = \rightarrow \) then \( H; c; pc; \ell \not\models pc \models \nabla(H^\approx) - H^\approx \)

b) if \( \pi = \leftarrow \) then \( H; c; pc; \ell \not\models pc \models (\ell - H)^\approx \)

Then for all attacks \( \delta_1 \) and \( \delta_2 \) such that Π; Γ; pc \models e[\psi] \; \text{says} \; \text{bool}, if \( e[\psi] \models \psi \rightarrow^* v_1 \), then \( v_1 = v_2 \).

**Proof.** Using HOL and Lemmas 2 and 11. See the technical report [29] for details.

**Theorem 2.** (Robust declassification). Let \( e[\psi] \) be a program such that

1) \( \Pi; \pi; pc \models e[\psi] ; \psi \models \text{bool} \)

2) \( H; c; pc; \ell \models pc \models (\ell - H)^\approx \)

Then for all attacks \( \delta_1 \) and \( \delta_2 \) and all inputs \( v \) such that Π, Γ, x, s, pc \models e[\psi] \; \text{says} \; \text{bool} and Π, Γ, pc \not\models v : s, if \( e[\psi] \models [x \rightarrow v] \rightarrow^* v'_1 \), then \( v'_1 = v'_2 \).

**Proof.** Let \( e'[\psi] \equiv e[\psi][x \rightarrow v] \), and let \( \delta'_1 = \delta'_2[\psi \rightarrow v] \). By Lemma 5, Π, Γ, pc \models e[\psi] ; \psi \models \text{bool}. Thus by Lemma 12 \( v'_1 = v'_2 \).

**Appendix B**

**Commitment Scheme Verification**

To prove the desired properties of commitment schemes for boolean values, let \( s = \text{bool} \) and recall:

\[ \Gamma_c = \text{commit, receive, open, } x : p \rightarrow \models s, y : p \land q^\approx \models s \]

- \( q \) cannot receive a value that hasn’t been committed. Let \( H = p^\approx \land q^\approx \). For any \( e \) and \( \Gamma_c \models pc_q \models e \models (p \land q^\approx) \models \text{says} \; \text{bool} \), observe that \( \Pi; pc_q \models H \not\models \psi \rightarrow \models \text{bool} \), \( \Pi; pc_q \not\models H^\approx \subseteq p^\approx \), \( \Pi; pc_q ; pc \models H^\approx \subseteq (p \land q^\approx)^\approx \), and \( \Pi; pc_q \models pc \models pc_q \models (p \land q^\approx)^\approx \). Therefore, by Theorem 1, if \( e[\psi] \models [x \rightarrow v_1] \rightarrow^* v'_1 \) and \( e[\psi] \models [x \rightarrow v_2] \rightarrow^* v'_2 \), then \( v'_1 \simeq v'_2 \).

- \( q \) cannot learn a value that hasn’t been opened. Let \( H = p^\approx \land q^\approx \). For any \( e \), \( \ell \), and \( \Gamma_c \models pc_q \models e \models (p \land q^\approx) \models \psi \models \text{says} \; \text{bool} \), observe that both \( \Pi; pc_q \models H \not\models \psi \rightarrow \models \text{bool} \) and \( \Pi; pc_q \not\models H \not\models p \land q^\approx \models \text{says} \; \text{bool} \). Therefore, Theorem 1 applies as above for both \( x \) and \( y \).

Thus if \( e[\psi] \models [x \rightarrow v_1] \rightarrow^* v'_1 \) and \( e[\psi] \models [x \rightarrow v_2] \rightarrow^* v'_2 \), then \( v'_1 \simeq v'_2 \), and if \( e[\psi] \models [x \rightarrow v_1] \rightarrow^* v'_1 \) and \( e[\psi] \models [x \rightarrow v_2] \rightarrow^* v'_2 \), then \( v'_1 \simeq v'_2 \).

- \( p \) cannot open a value that hasn’t been received. Let \( H = p^\approx \land q^\approx \). For any \( e \) and \( \Gamma_c \models pc_p \models e \models (p \land q^\approx) \models \psi \models \text{says} \; \text{bool} \), observe that \( \Pi; pc_p \models H \not\models p^\approx \models \text{says} \; \text{bool} \), \( \Pi; pc_p ; pc \not\models H^\approx \subseteq (p \land q^\approx)^\approx \), and \( \Pi; pc_p ; pc \models pc_p \models (p \land q^\approx)^\approx \). Therefore, by Theorem 1, if \( e[\psi] \models [x \rightarrow v_1] \rightarrow^* v'_1 \) and \( e[\psi] \models [x \rightarrow v_2] \rightarrow^* v'_2 \), then \( v'_1 \simeq v'_2 \).