

# Principal-Centric Reasoning in Constructive Authorization Logic

Deepak Garg

Carnegie Mellon University

June 23, 2008

# Outline

1 Background

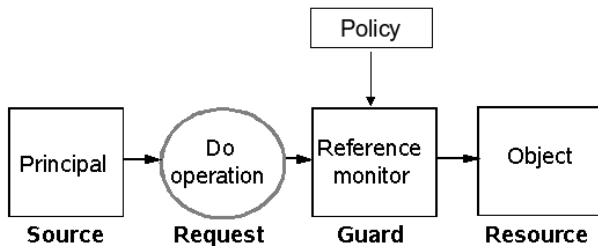
2 Logic design: proof-theory

# Outline

1 Background

2 Logic design: proof-theory

# Broad Setting: The Problem of Access Control



Source: Lampson et al. '92

- Policy is central – how do we represent it?
  - ▶ Common methods: bit-level encodings, access control lists
  - ▶ Low-level, confusing; may lead to programming and administrative errors
- Represent policies as formulas in a logic
  - ▶ Rigorous, high-level, flexible
  - ▶ Can we use the logical representation for enforcement?
  - ▶ What logic should be we use?

# Enforcement through Proofs

- Allow access iff there is a formal **proof** [Blaze *et al.* '96]
- Let  $\Gamma$  denote the set of formulas representing policies
- Allow access iff  $\Gamma \vdash A$  ( $A$  depends on requester, object, and operation)
  
- Who constructs the proof?
- Put burden of proof construction on requesting principal
  - ▶ Proof-carrying authorization [Appel, Felten '99]
- Requester **constructs** and submits proof with request
- Reference monitor **verifies** proof
  - ▶ Proof good  $\Rightarrow$  allow access
  - ▶ Proof bad  $\Rightarrow$  deny access

**Proofs are a generic enforcement mechanism** for access control

# Which Logic?

- **First-order/propositional** vs. higher-order
- **Intuitionistic** vs. classical
- Does first-order intuitionistic logic suffice?
- Almost, but some policy motifs need other constructs

# Which Logic?

- **First-order/propositional** vs. higher-order
- **Intuitionistic** vs. classical
  
- Does first-order intuitionistic logic suffice?
  
- Almost, but some policy motifs need other constructs

# Which Logic?

- **First-order/propositional** vs. higher-order
- **Intuitionistic** vs. classical
  
- Does first-order intuitionistic logic suffice?
  
- Almost, but some policy motifs need other constructs

# Decentralization: The Need for Modalities

- Policies may be made by different principals
  - Example (Can Alice visit USA? [without a visa])
    - 1 “Any Canadian national may visit USA without a visa”
    - 2 “Alice is a Canadian national”
  - Policy (1) made by USA; policy (2) made by Canada
  - How do we represent the difference?
- 
- $K$  says  $A$  (principal  $K$  states that formula  $A$  is true)
  - Family of principal-indexed modalities [Lampson *et al.* '92]
  - Example
    - 1 USA says  $\forall i. ((\text{Canada says } \text{myCitizen}(i)) \supset \text{mayVisit}(i))$
    - 2 Canada says  $\text{myCitizen}(\text{Alice})$

Which modal logic?

# Decentralization: The Need for Modalities

- Policies may be made by different principals
- Example (Can Alice visit USA? [without a visa])
  - 1 "Any Canadian national may visit USA without a visa"
  - 2 "Alice is a Canadian national"
- Policy (1) made by USA; policy (2) made by Canada
- How do we represent the difference?
  
- $K$  says  $A$  (principal  $K$  states that formula  $A$  is true)
- Family of principal-indexed modalities [Lampson *et al.* '92]
- Example
  - 1 USA says  $\forall i. ((\text{Canada says myCitizen}(i)) \supset \text{mayVisit}(i))$
  - 2 Canada says  $\text{myCitizen}(\text{Alice})$

Which modal logic?

# Decentralization: The Need for Modalities

- Policies may be made by different principals
- Example (Can Alice visit USA? [without a visa])
  - 1 “Any Canadian national may visit USA without a visa”
  - 2 “Alice is a Canadian national”
- Policy (1) made by USA; policy (2) made by Canada
- How do we represent the difference?
  
- $K$  says  $A$  (principal  $K$  states that formula  $A$  is true)
- Family of principal-indexed modalities [Lampson *et al.* '92]
- Example
  - 1 USA says  $\forall i. ((\text{Canada says } \text{myCitizen}(i)) \supset \text{mayVisit}(i))$
  - 2 Canada says  $\text{myCitizen}(\text{Alice})$

Which modal logic?

# Choosing the “Right” $K$ says $A$

- Trade-off between
  - ▶ Weak modalities (useless), e.g., treat  $K$  says  $A$  syntactically
  - ▶ Strong modalities (dangerous), e.g., assume  $A \equiv (K \text{ says } A)$

- Some past approaches:

- ▶  $\Box$  from modal logic  $K$  (classical) [Lampson *et al.* '92, '93]

$$\frac{\vdash A}{\vdash K \text{ says } A} \quad (\text{nec})$$
$$\vdash (K \text{ says } (A \supset B)) \supset ((K \text{ says } A) \supset (K \text{ says } B)) \quad (K)$$

- ▶ Original PCA (classical) [Appel, Felten '99]

$$\vdash A \supset (K \text{ says } A) \quad (\text{unit})$$
$$\vdash (K \text{ says } (A \supset B)) \supset ((K \text{ says } A) \supset (K \text{ says } B)) \quad (K)$$

- ▶  $\bigcirc$  from lax logic (intuitionistic) [GF '06, Abadi '06, ...]

$$\vdash A \supset (K \text{ says } A) \quad (\text{unit})$$
$$\vdash (K \text{ says } (A \supset B)) \supset ((K \text{ says } A) \supset (K \text{ says } B)) \quad (K)$$
$$\vdash (K \text{ says } K \text{ says } A) \supset (K \text{ says } A) \quad (C4)$$

▶ ...

- No clear metric to evaluate “fitness” of modality

# Choosing the “Right” $K$ says $A$

- Trade-off between

- ▶ Weak modalities (useless), e.g., treat  $K$  says  $A$  syntactically
- ▶ Strong modalities (dangerous), e.g., assume  $A \equiv (K \text{ says } A)$

- Some past approaches:

- ▶  $\square$  from modal logic  $K$  (classical) [Lampson *et al.* '92, '93]

$$\frac{\vdash A}{\vdash K \text{ says } A} \quad (\text{nec})$$
$$\vdash (K \text{ says } (A \supset B)) \supset ((K \text{ says } A) \supset (K \text{ says } B)) \quad (K)$$

- ▶ Original PCA (classical) [Appel, Felten '99]

$$\vdash A \supset (K \text{ says } A) \quad (\text{unit})$$
$$\vdash (K \text{ says } (A \supset B)) \supset ((K \text{ says } A) \supset (K \text{ says } B)) \quad (K)$$

- ▶  $\bigcirc$  from lax logic (intuitionistic) [GF '06, Abadi '06, ...]

$$\vdash A \supset (K \text{ says } A) \quad (\text{unit})$$
$$\vdash (K \text{ says } (A \supset B)) \supset ((K \text{ says } A) \supset (K \text{ says } B)) \quad (K)$$
$$\vdash (K \text{ says } K \text{ says } A) \supset (K \text{ says } A) \quad (C4)$$

- ▶ ...

- No clear metric to evaluate “fitness” of modality

## In this paper . . .

- A new propositional logic  $DTL_0$  for representing access control policies
  - ▶ Sequent calculus and Hilbert-style axiomatization
  - ▶ Meta-theory: cut-elimination
  - ▶ Kripke semantics
  - ▶ Translations from other authorization logics to  $DTL_0$
  - ▶ Closely related to constructive S4
- Emphasis on proof-theory esp. sequent calculus and cut-elimination
  - ▶ Proofs central to enforcement
  - ▶ Assurance of the logic's soundness (*à la* Martin-Löf's type-theory)

## In this paper . . .

- A new propositional logic  $DTL_0$  for representing access control policies
  - ▶ Sequent calculus and Hilbert-style axiomatization
  - ▶ Meta-theory: cut-elimination
  - ▶ Kripke semantics
  - ▶ Translations from other authorization logics to  $DTL_0$
  - ▶ Closely related to constructive S4
- Emphasis on proof-theory esp. sequent calculus and cut-elimination
  - ▶ Proofs central to enforcement
  - ▶ Assurance of the logic's soundness (*à la* Martin-Löf's type-theory)

# Outline

1 Background

2 Logic design: proof-theory

# DTL<sub>0</sub>: Syntax and Axiomatic System

$$A, B ::= P \mid A \wedge B \mid A \vee B \mid \top \mid \perp \mid A \supset B \mid K \text{ says } A$$

## Axiomatic System

$\frac{\vdash A}{\vdash K \text{ says } A}$	(nec)
$\vdash (K \text{ says } (A \supset B)) \supset ((K \text{ says } A) \supset (K \text{ says } B))$	(K)
$\vdash (K \text{ says } A) \supset (K \text{ says } K \text{ says } A)$	(4)
$\vdash K \text{ says } ((K \text{ says } A) \supset A)$	(C)

- (C) stands for “conceit”
- Replacing (C) with  $(K \text{ says } A) \supset A$  gives CS4

# Sequent Calculus

- Follow Martin-Löf's method: separate formulas from judgments
  - ▶ Judgments are predicates over formulas, and evidenced by proofs
- Categorical (non-hypothetical) judgments:
  - ▶  $A$  **true** (Usually elide the name **true**)
  - ▶  $K$  **claims**  $A$  ( $K$  **claims**  $A \equiv (K$  **says**  $A)$  **true**)
  - ▶  $K$  **says**  $A$  internalizes  $K$  **claims**  $A$  into the syntax of formulas
- Hypothetical judgments or sequents:  $\boxed{\Gamma \xrightarrow{K} A \text{ true}}$   
 $\Gamma ::= \cdot \mid \Gamma, A \text{ true} \mid \Gamma, K \text{ claims } A$
- "If we assume that  $K$  **claims**  $A$  implies  $A$  for each  $A$ , then assumptions  $\Gamma$  entail  $A$ "
  - ▶  $K$  is called the **context** of the sequent

# Basic Principles

- Context principle: In context  $K$ ,  $K$  **claims**  $A$  entails  $A$  **true**
- Claim principle:  $K$  **claims**  $A$  holds (in any context) if using only claims of  $K$ , we can prove  $A$  **true** in context  $K$ .
- Internalization principle:  $K$  **claims**  $A$  is equivalent to  $(K$  **says**  $A)$  **true**

# Basic Rules

$$\frac{}{\Gamma, P \text{ true} \xrightarrow{K} P \text{ true}} \text{init}$$

$$\frac{\Gamma, K \text{ claims } A, A \text{ true} \xrightarrow{K} C \text{ true}}{\Gamma, K \text{ claims } A \xrightarrow{K} C \text{ true}} \text{claims}$$

Context principle: In context  $K$ ,  $K$  claims  $A$  entails  $A$  true

## Rules for implication

$$\frac{\Gamma, A \text{ true} \xrightarrow{K} B \text{ true}}{\Gamma \xrightarrow{K} (A \supset B) \text{ true}} \supset R$$

$$\frac{\Gamma, (A \supset B) \text{ true} \xrightarrow{K} A \text{ true} \quad \Gamma, B \text{ true} \xrightarrow{K} C \text{ true}}{\Gamma, (A \supset B) \text{ true} \xrightarrow{K} C \text{ true}} \supset L$$

- Rules for other propositional connectives as usual

## Rules for says

$$\frac{\Gamma|_K \xrightarrow{K} A \text{ true}}{\Gamma \xrightarrow{K'} (K \text{ says } A) \text{ true}} \text{saysR}$$

where  $\Gamma|_K = \{K \text{ claims } C \mid (K \text{ claims } C) \in \Gamma\}$

$$\frac{\Gamma, (K \text{ says } A) \text{ true}, K \text{ claims } A \xrightarrow{K'} C \text{ true}}{\Gamma, (K \text{ says } A) \text{ true} \xrightarrow{K'} C \text{ true}} \text{saysL}$$

Internalization principle:  $K \text{ claims } A$  is equivalent to  $(K \text{ says } A) \text{ true}$

Claim principle:  $K \text{ claims } A$  holds (in any context) if using only claims of  $K$ , we can prove  $A \text{ true}$  in context  $K$ .

# Summary of Rules

$$\frac{}{\Gamma, P \text{ true} \xrightarrow{K} P \text{ true}} \text{init}$$

$$\frac{\Gamma, K \text{ claims } A, A \text{ true} \xrightarrow{K} C \text{ true}}{\Gamma, K \text{ claims } A \xrightarrow{K} C \text{ true}} \text{claims}$$

$$\frac{\Gamma, A \text{ true} \xrightarrow{K} B \text{ true}}{\Gamma \xrightarrow{K} (A \supset B) \text{ true}} \supset R$$

$$\frac{\Gamma, (A \supset B) \text{ true} \xrightarrow{K} A \text{ true} \quad \Gamma, B \text{ true} \xrightarrow{K} C \text{ true}}{\Gamma, (A \supset B) \text{ true} \xrightarrow{K} C \text{ true}} \supset L$$

$$\frac{\Gamma |_K \xrightarrow{K} A \text{ true}}{\Gamma \xrightarrow{K'} (K \text{ says } A) \text{ true}} \text{saysR}$$

$$\frac{\Gamma, (K \text{ says } A) \text{ true}, K \text{ claims } A \xrightarrow{K'} C \text{ true}}{\Gamma, (K \text{ says } A) \text{ true} \xrightarrow{K'} C \text{ true}} \text{saysL}$$

# Properties and Meta-Theory

- Admissibility of cut:
  - ▶  $\Gamma \xrightarrow{K} A \text{ true}$  and  $\Gamma, A \text{ true} \xrightarrow{K} C \text{ true}$  imply  $\Gamma \xrightarrow{K} C \text{ true}$
- Identity:
  - ▶  $\Gamma, A \text{ true} \xrightarrow{K} A \text{ true}$
- Connection between axiomatic system and sequent calculus
  - ▶  $\Gamma \xrightarrow{K} A$  if and only if  $\vdash K \text{ says } (\Gamma \supset A)$
  - ▶ Actually an *embedding theorem*
- Sound and complete Kripke semantics in the paper
  - ▶ Adapt Alechina *et al.*'s Kripke semantics for CS4
  - ▶ No  $\diamond$ ; need to associate principals with worlds
- Sound and complete translations from other authorization logics

# DTL<sub>0</sub> Generalizes CS4 (Without $\diamond$ )

- In the special case of only one principal (say  $\ell$ ), DTL<sub>0</sub>'s sequent calculus reduces to that for CS4.

$$\frac{}{\Gamma, P \text{ true} \xrightarrow{K} P \text{ true}} \text{init}$$

$$\frac{\Gamma, K \text{ claims } A, A \text{ true} \xrightarrow{K} C \text{ true}}{\Gamma, K \text{ claims } A \xrightarrow{K} C \text{ true}} \text{claims}$$

$$\frac{\Gamma, A \text{ true} \xrightarrow{K} B \text{ true}}{\Gamma \xrightarrow{K} (A \supset B) \text{ true}} \supset R$$

$$\frac{\Gamma, (A \supset B) \text{ true} \xrightarrow{K} A \text{ true} \quad \Gamma, B \text{ true} \xrightarrow{K} C \text{ true}}{\Gamma, (A \supset B) \text{ true} \xrightarrow{K} C \text{ true}} \supset L$$

$$\frac{\Gamma |_{K} \xrightarrow{K} A \text{ true}}{\Gamma \xrightarrow{K'} (K \text{ says } A) \text{ true}} \text{saysR}$$

$$\frac{\Gamma, (K \text{ says } A) \text{ true}, K \text{ claims } A \xrightarrow{K'} C \text{ true}}{\Gamma, (K \text{ says } A) \text{ true} \xrightarrow{K'} C \text{ true}} \text{saysL}$$

# DTL<sub>0</sub> Generalizes CS4 (Without $\diamond$ )

- In the special case of only one principal (say  $\ell$ ), DTL<sub>0</sub>'s sequent calculus reduces to that for CS4.

$$\frac{}{\Gamma, P \text{ true} \xrightarrow{\ell} P \text{ true}} \text{init}$$

$$\frac{\Gamma, \ell \text{ claims } A, A \text{ true} \xrightarrow{\ell} C \text{ true}}{\Gamma, \ell \text{ claims } A \xrightarrow{\ell} C \text{ true}} \text{claims}$$

$$\frac{\Gamma, A \text{ true} \xrightarrow{\ell} B \text{ true}}{\Gamma \xrightarrow{\ell} (A \supset B) \text{ true}} \supset R$$

$$\frac{\Gamma, (A \supset B) \text{ true} \xrightarrow{\ell} A \text{ true} \quad \Gamma, B \text{ true} \xrightarrow{\ell} C \text{ true}}{\Gamma, (A \supset B) \text{ true} \xrightarrow{\ell} C \text{ true}} \supset L$$

$$\frac{\Gamma |_{\ell} \xrightarrow{\ell} A \text{ true}}{\Gamma \xrightarrow{\ell} (\ell \text{ says } A) \text{ true}} \text{saysR}$$

$$\frac{\Gamma, (\ell \text{ says } A) \text{ true}, \ell \text{ claims } A \xrightarrow{\ell} C \text{ true}}{\Gamma, (\ell \text{ says } A) \text{ true} \xrightarrow{\ell} C \text{ true}} \text{saysL}$$

## DTL<sub>0</sub> Generalizes CS4 (Without $\diamond$ )

- In the special case of only one principal (say  $\ell$ ), DTL<sub>0</sub>'s sequent calculus reduces to that for CS4.

$$\frac{}{\Gamma, P \text{ true} \rightarrow P \text{ true}} \text{init}$$

$$\frac{\Gamma, A \text{ valid}, A \text{ true} \rightarrow C \text{ true}}{\Gamma, A \text{ valid} \rightarrow C \text{ true}} \text{valid}$$

$$\frac{\Gamma, A \text{ true} \rightarrow B \text{ true}}{\Gamma \rightarrow (A \supset B) \text{ true}} \supset R$$

$$\frac{\Gamma, (A \supset B) \text{ true} \rightarrow A \text{ true} \quad \Gamma, B \text{ true} \rightarrow C \text{ true}}{\Gamma, (A \supset B) \text{ true} \rightarrow C \text{ true}} \supset L$$

$$\frac{\Gamma \mid \rightarrow A \text{ true}}{\Gamma \rightarrow (\Box A) \text{ true}} \Box R$$

$$\frac{\Gamma, (\Box A) \text{ true}, A \text{ valid} \rightarrow C \text{ true}}{\Gamma, (\Box A) \text{ true} \rightarrow C \text{ true}} \Box L$$

# DTL<sub>0</sub> $\Rightarrow$ CS4<sup>m</sup>

- The following embedding is sound and complete

$$\ulcorner K \text{ says } A \urcorner = \Box_K(g_K \supset \ulcorner A \urcorner)$$

- (CS4<sup>m</sup>  $\Rightarrow$  DTL<sub>0</sub>) Unknown!

# Summary and Future Work

- New logic for writing authorization policies
- Unusual, but expressive and (hopefully) useful
- Emphasis on proof-theory; sequent calculus, meta-theoretic properties
- Kripke semantics
- Connections to other logics
  
- Part of a larger project
  - ▶ More logical primitives: linearity, time
  - ▶ Applications to real policies
  - ▶ Implementation of a file system using the logic
  - ▶ Using proof-theory to prove properties of policies

# Thank You

Questions?

# Rules without judgments

$$\frac{}{\Gamma, P \xrightarrow{K} P} \text{init} \quad \frac{\Gamma, A \xrightarrow{K} B}{\Gamma \xrightarrow{K} A \supset B} \supset R \quad \frac{\Gamma, A \supset B \xrightarrow{K} A \quad \Gamma, B \xrightarrow{K} C}{\Gamma, A \supset B \xrightarrow{K} C} \supset L$$
$$\frac{K \text{ says } \Gamma \xrightarrow{K} A}{K \text{ says } \Gamma, \Gamma' \xrightarrow{K'} K \text{ says } A} \text{saysR} \quad \frac{\Gamma, K \text{ says } A, A \xrightarrow{K} C}{\Gamma, K \text{ says } A \xrightarrow{K} C} \text{saysL}$$