An Authorization Logic with Explicit Time

Henry DeYoung, Deepak Garg, and Frank Pfenning

Computer Science Department
Carnegie Mellon University

Computer Security Foundations 2008
June 24, 2008

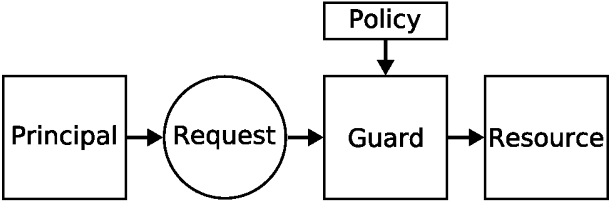
Outline

Outline

Outline

Outline

The Problem of Access Control



Source: [Lampson *et al.* '92]

- Problem
  - Restrict access to a resource according to *policy*.
- Approach
  - Specify (and enforce) policies using an *authorization logic*.

Logic for Access Control

Policies are expressed as logical theories. [LABW ’92]

Benefits:

- Precision
  - Logical specifications are more precise than natural language.
- Flexibility
  - Can incorporate user-defined predicates.
  - Can easily change policies without changing the system.
- Enforcement via PCA [AF ’99, Bauer ’03]
  - Allow access to a resource if and only if a formal proof of access is presented.
- Policy Analysis
  - Consequence of proof-theory.
  - E.g., non-interference theorems. [GP ’06, Abadi ’06]

Outline

Motivating Example: Office Entry

Setting:

- admin, who controls entry to academic offices.
- Alice, a professor.
- Bob, a graduate student of Alice.

Policy:

- During 2007–2008, the admin allows a person K_1 to enter an office owned by a person K_2, provided that K_2 has authorized K_1 to enter.

Dilemma:

- Alice is at CSF this week.
- Bob needs a book from Alice's office.

A Traditional Approach to Time-Dependent Policies

Traditional approach:

- Ignore time-dependencies in the logical formulation of the policy.
- Policy:

$$\mathrm{admin}\ \textsf{says}\ (\forall K_1.\forall K_2.((K_2\ \textsf{says}\ \texttt{may\_enter}(K_1, K_2)) \supset \texttt{may\_enter}(K_1, K_2)))$$

- Alice signs a certificate allowing Bob to enter during the week 6/23/08–6/30/08.

$$\mathrm{Alice}\ \textsf{says}\ \texttt{may\_enter}(\mathrm{Bob}, \mathrm{Alice})$$

- Bob tries to enter at 1pm 6/24/08. He must prove:

$$\mathrm{admin}\ \textsf{says}\ \texttt{may\_enter}(\mathrm{Bob}, \mathrm{Alice})$$

- Credentials used in the proof are checked for expiration.

Drawbacks:

- Correct proofs might be rejected because of expired credentials.
- Cannot analyze time using logical methods.

A Better Approach to Time-Dependent Policies

Better approach:

- Include time in the logic.
- Policy:

$$(\mathrm{admin}\ \textsf{says}\ (\forall K_1.\forall K_2.((K_2\ \textsf{says}\ \texttt{may\_enter}(K_1, K_2)) \supset \texttt{may\_enter}(K_1, K_2)))) \ @\ [2007, 2008]$$

- Alice signs a certificate allowing Bob to enter during the week 6/23/08–6/30/08.

$$(\mathrm{Alice}\ \textsf{says}\ \texttt{may\_enter}(\mathrm{Bob}, \mathrm{Alice}))\ @\ [6/23/08, 6/30/08]$$

- Bob tries to enter at 1pm 6/24/08. He must prove:

$$(\mathrm{admin}\ \textsf{says}\ \texttt{may\_enter}(\mathrm{Bob}, \mathrm{Alice}))\ @\ [\text{1pm } 6/24/08, \text{1pm } 6/24/08]$$

Benefits:

- Proof construction is accurate with respect to time.
- Analysis of time-dependent policies.

Purpose of the Paper

- Design an authorization logic (for use with PCA) in which time-dependent policies can be specified and enforced.
- Hence, we propose η logic (explicit time authorization logic).

Outline

Key Ideas of η Logic

Key Ideas:

- Intuitionistic sequent calculus.
- All truths and statements are relativized to a set of time points.
- Authorization policies use *absolute, specific* sets of time.
  - Temporal logic seems inadequate.
  - For convenience, sets of time are called “intervals”.
- Model explicit time with hybrid @.
  - Hybrid logic: modal logic where worlds may appear in formulas.
  - Worlds $\cong$ intervals.
- Abstract away from “implementation” of times and sets of time.
  - Require only a partial order of inclusion on intervals.
- Constraints for modeling the usual inclusion ordering on intervals.

Syntax and Basic Judgments

Syntax:

$$A, B ::= K \text{ says } A \mid A \mathbin{@} I \mid P \mid A \supset B \mid \forall x{:}s.A \mid \ \ldots$$

Martin-Löf: Judgments are the objects of knowledge and evidenced by proofs. Propositions are the subjects of judgments.

Basic Judgments:

1. $A[I]$: A is true on I.
   - Judgmental form of $A \mathbin{@} I$.
2. (K affirms A) at I: During I, K affirms that A is true on I.
   - Judgmental form of (K says A) $\mathbin{@} I$.

Hypothetical Judgments

Hypotheses:

- Ψ contains $I \supseteq I'$ constraint hypotheses
- Γ contains $A[I]$ hypotheses

Hypothetical Judgments:

1. $\Psi \models I \supseteq I'$
2. $\Psi; \Gamma \Longrightarrow A[I]$
3. $\Psi; \Gamma \Longrightarrow (K \text{ affirms } A) \text{ at } I$

Outline

Inference Rules: Hypothetical Judgments

$$\frac{\Psi \models I \supseteq I' \quad (P \text{ atomic})}{\Psi; \Gamma, P[I] \Longrightarrow P[I']}\ \text{init}$$

Inference Rules: @ as a Hybrid Connective

$$\frac{\Psi ; \Gamma \Longrightarrow A[I]}{\Psi ; \Gamma \Longrightarrow (A \mathbin{@} I)[I']}\ @R \qquad \frac{\Psi ; \Gamma, (A \mathbin{@} I)[I'], A[I] \Longrightarrow \gamma}{\Psi ; \Gamma, (A \mathbin{@} I)[I'] \Longrightarrow \gamma}\ @L$$

Admissible properties:

- Write $\vdash A$ if $\cdot ; \cdot \Longrightarrow A[I'']$ for all I'' and all instantiations of the propositional variables. Write $\nvdash A$ otherwise.

1. $\nvdash (A \mathbin{@} I) \supset (A \mathbin{@} I')$ (in general)
2. $\vdash (A \mathbin{@} I) \supset (A \mathbin{@} I')$ if $\cdot \models I \supseteq I'$
3. $\vdash (A \mathbin{@} I \mathbin{@} I') \equiv (A \mathbin{@} I)$

Inference Rules: $\supset$

$$\frac{\Psi, I \supseteq i; \Gamma, A[i] \Longrightarrow B[i] \quad (i \text{ fresh})}{\Psi; \Gamma \Longrightarrow (A \supset B)[I]} \supset R$$

$$\frac{\Psi \models I \supseteq I' \quad \Psi; \Gamma, (A \supset B)[I] \Longrightarrow A[I'] \quad \Psi; \Gamma, (A \supset B)[I], B[I'] \Longrightarrow \gamma}{\Psi; \Gamma, (A \supset B)[I] \Longrightarrow \gamma} \supset L$$

1. $\vdash ((A \supset B) @ I) \supset ((A @ I) \supset (B @ I))$
2. $\not\vdash ((A @ I) \supset (B @ I)) \supset ((A \supset B) @ I)$

Inference Rules: says as a K-Indexed Monad

$$\frac{\Psi;\Gamma \Longrightarrow A[I]}{\Psi;\Gamma \Longrightarrow (K \text{ affirms } A) \text{ at } I}\ \text{affirms}$$

$$\frac{\Psi;\Gamma \Longrightarrow (K \text{ affirms } A) \text{ at } I}{\Psi;\Gamma \Longrightarrow (K \text{ says } A)[I]}\ \text{says}R$$

$$\frac{\Psi;\Gamma,(K \text{ says } A)[I], A[I] \Longrightarrow (K \text{ affirms } B) \text{ at } I' \quad \Psi \models I \supseteq I'}{\Psi;\Gamma,(K \text{ says } A)[I] \Longrightarrow (K \text{ affirms } B) \text{ at } I'}\ \text{says}L$$

1. $\vdash A \supset (K \text{ says } A)$
2. $\vdash (K \text{ says } (A \supset B)) \supset ((K \text{ says } A) \supset (K \text{ says } B))$
3. $\vdash (K \text{ says } (K \text{ says } A)) \supset (K \text{ says } A)$
4. $\not\vdash (K \text{ says } A) \supset A$
5. $\not\vdash ((K \text{ says } A) \mathbin{@} I) \supset (K \text{ says } (A \mathbin{@} I))$
6. $\not\vdash (K \text{ says } (A \mathbin{@} I)) \supset ((K \text{ says } A) \mathbin{@} I)$

Outline

Meta-theory

Theorem (Admissibility of Cut)

If $\Psi; \Gamma \Longrightarrow A[I]$ *and* $\Psi; \Gamma, A[I] \Longrightarrow \gamma$, *then* $\Psi; \Gamma \Longrightarrow \gamma$.

- Entails the subformula property.
- Consequently, the connectives are defined *entirely* by their left and right rules.

Theorem (Subsumption)

If $\Psi; \Gamma \Longrightarrow A[I]$ *and* $\Psi \models I \supseteq I'$, *then* $\Psi; \Gamma \Longrightarrow A[I']$.

- Verifies desirable behavior of intervals.
- Verifies a proper fit between constraint and logical reasoning.

Outline

PCA with η Logic

Principals state policies by digitally signing certificates.

When a principal requests access to a resource:

1. The certificates are converted to logical assumptions Γ; validity bounds I are converted to $@\, I$ in Γ.
2. The principal must submit a proof of
$$\cdot; \Gamma \Longrightarrow A_{\text{access}}[\text{now}, \text{now} + \epsilon]$$
where:
   - A_{access} is the required formula to access the resource
   - (By subsumption, it is sufficient to prove
   $$\cdot; \Gamma \Longrightarrow A_{\text{access}}[I]$$
   for any I such that $\cdot \models I \supseteq [\text{now}, \text{now} + \epsilon]$.)
3. Access is granted if and only if the proof is correct.

Proof construction is now correct with respect to time.

Modeling Consumable Credentials

Problem:

- As presented in this talk, η logic cannot model consumable credentials.
- Alice probably wants Bob to enter *at most once* during the week 6/23/08–6/30/08.

Solution:

- In our paper, η logic incorporates linear logic to express "use-once" authorizations.
  - Follows previous work on linear authorization logics (without time). [GBBPR '06, CCDEdHL '06, BM '06]
- Example, inference rules, admissible properties, and meta-theory all easily extend to the linear case (see paper).

Outline

Future Work and Summary

Future work:

- Formal comparison of η logic to other logics and languages.
- Implementation of a PCA architecture based on η logic.
- Extend non-interference theorems to η logic. [GP '06, Abadi '06]

Summary:

- Using logic for access control provides several benefits.
- If the logic does not include time, benefits cannot apply to time.
- Therefore, we propose η logic.
  - Incorporates time internally using a hybrid @ connective.
  - Possesses "nice" meta-theoretic properties such as admissibility of cut.
  - Can be extended to model consumable credentials.

Thank you!

Questions?

Intuitionistic vs. Classical Logic

- Keep the logic constructive to make evidence as direct as possible.
  - Key role of proofs in the system.
- In classical logic, $\neg\neg A \supset A$ holds.
  - If there is no proof of access denial ($\neg\neg A$), then there is a proof of access (A).
  - Risky for security purposes: a proof of denial might have been overlooked.
- In constructive logic, $\neg\neg A \supset A$ is not provable.

Adding Linearity

Refine basic judgments:

1. $A[I]$: *Single-use* resource A is true on I.
2. $A[\![I]\!]$: *Multi-use* fact A is true on I.
3. (K affirms A) at I: During I, K affirms that *single-use* resource A is true on I.

Refine hypothetical judgments:

1. $\Psi; \Gamma; \Delta \Longrightarrow A[I]$
2. $\Psi; \Gamma; \Delta \Longrightarrow (K \text{ affirms } A) \text{ at } I$

$$\frac{\Psi \models I \supseteq I'}{\Psi; \Gamma; P[I] \Longrightarrow P[I']}\ \text{init} \qquad \frac{\Psi; \Gamma, A[\![I]\!]; \Delta, A[I] \Longrightarrow \gamma}{\Psi; \Gamma, A[\![I]\!]; \Delta \Longrightarrow \gamma}\ \text{copy}$$

Inference Rules: $\wedge$

$$\frac{\Psi; \Gamma \Longrightarrow A[I] \quad \Psi; \Gamma \Longrightarrow B[I]}{\Psi; \Gamma \Longrightarrow (A \wedge B)[I]} \wedge R$$

$$\frac{\Psi; \Gamma, (A \wedge B)[I], A[I] \Longrightarrow \gamma}{\Psi; \Gamma, (A \wedge B)[I] \Longrightarrow \gamma} \wedge L_1 \qquad \frac{\Psi; \Gamma, (A \wedge B)[I], B[I] \Longrightarrow \gamma}{\Psi; \Gamma, (A \wedge B)[I] \Longrightarrow \gamma} \wedge L_2$$

1. $\vdash ((A \wedge B) @ I) \equiv ((A @ I) \wedge (B @ I))$

Meta-theory: Identity

Theorem (Identity)

For all A, if $\Psi \models I \supseteq I'$, then $\Psi; \Gamma, A[I] \Longrightarrow A[I']$.

- Generalizes the init rule to compound propositions.

Generic Non-Interference Theorem

- If $\Psi;\Gamma, A[I] \Longrightarrow B[I']$ and $\langle$some criteria on Ψ, Γ, A, I, B, $I'\rangle$, then $\Psi;\Gamma \Longrightarrow B[I']$.