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

1 Background
   - Motivating Example
Outline

1. Background
   - Motivating Example

2. $\eta$ Logic
   - Key Ideas and Judgments
   - Inference Rules and Admissible Properties
   - Meta-theory
Outline

1 Background
   - Motivating Example

2 $\eta$ Logic
   - Key Ideas and Judgments
   - Inference Rules and Admissible Properties
   - Meta-theory

3 Proof-Carrying Authorization (PCA) and Linearity
Outline

1 Background
   ■ Motivating Example

2 $\eta$ Logic
   ■ Key Ideas and Judgments
   ■ Inference Rules and Admissible Properties
   ■ Meta-theory

3 Proof-Carrying Authorization (PCA) and Linearity

4 Conclusion
The Problem of Access Control

- Problem
  - Restrict access to a resource according to *policy*.

- Approach
  - Specify (and enforce) policies using an *authorization logic*.

Source: [Lampson et al. '92]
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]
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.
Traditional approach:

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

- Policy:

  \[
  \text{admin says} \ (\forall K_1.\forall K_2. ((K_2 \text{ says may}_\text{enter}(K_1, K_2)) \supset \text{may}_\text{enter}(K_1, K_2)))
  \]

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

  \[\text{Alice says may}_\text{enter}(\text{Bob, Alice})\]

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

  \[\text{admin says may}_\text{enter}(\text{Bob, Alice})\]

- 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:

\[
\text{admin says } (\forall K_1.\forall K_2.((K_2 \text{ says } \text{may}\_\text{enter}(K_1, K_2)) \supset \text{may}\_\text{enter}(K_1, K_2)))) @ [2007, 2008]
\]

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

\[
(Alice \text{ says } \text{may}\_\text{enter}(Bob, Alice)) @ [6/23/08, 6/30/08]
\]

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

\[
(\text{admin says } \text{may}\_\text{enter}(Bob, Alice)) @ [1pm 6/24/08, 1pm 6/24/08]
\]

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 $\eta$ logic (explicit time authorization logic).
Outline

1. Background
   - Motivating Example

2. Logic
   - Key Ideas and Judgments
   - Inference Rules and Admissible Properties
   - Meta-theory

3. Proof-Carrying Authorization (PCA) and Linearity

4. Conclusion
Key Ideas of $\eta$ 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:

\[ A, B ::= \textit{K says } A \mid A @ I \mid P \mid A \supset B \mid \forall x: s.A \mid \ldots \]

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 \( A @ I \).

2. \( (K \text{ affirms } A) \) at \( I \): During \( I \), \( K \) affirms that \( A \) is true on \( I \).
   - Judgmental form of \( (K \text{ says } A) @ I \).
Hypothetical Judgments

Hypotheses:
- \( \psi \) contains \( I \supseteq I' \) constraint hypotheses
- \( \Gamma \) contains \( A[I] \) hypotheses

Hypothetical Judgments:
1. \( \psi \models I \supseteq I' \)
2. \( \psi; \Gamma \models A[I] \)
3. \( \psi; \Gamma \models (K \text{ affirms } A) \text{ at } I \)
Outline

1 Background
   - Motivating Example

2 $\eta$ Logic
   - Key Ideas and Judgments
   - Inference Rules and Admissible Properties
   - Meta-theory

3 Proof-Carrying Authorization (PCA) and Linearity

4 Conclusion
Inference Rules: Hypothetical Judgments

\[ \Psi \models I \supseteq I' \quad (P \text{ atomic}) \]

\[ \frac{\Psi; \Gamma, P[I] \implies P[I']} {\init} \]
Inference Rules: @ as a Hybrid Connective

\[
\frac{\psi; \Gamma \Rightarrow A[I]}{\psi; \Gamma \Rightarrow (A \circ I)[I']} @R
\]

\[
\frac{\psi; \Gamma, (A \circ I)[I'], A[I] \Rightarrow \gamma}{\psi; \Gamma, (A \circ I)[I'] \Rightarrow \gamma} @L
\]

Admissible properties:

- **Write** \( \vdash A \) if \( \cdot; \cdot \Rightarrow A[I''] \) for all \( I'' \) and all instantiations of the propositional variables. Write \( \nvdash A \) otherwise.
  
  1. \( \nvdash (A \circ I) \supset (A \circ I') \) (in general)
  2. \( \vdash (A \circ I) \supset (A \circ I') \) if \( I \models I' \)
  3. \( \vdash (A \circ I \circ I') \equiv (A \circ I) \)
Inference Rules: ⊳

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

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

1. ⊳ (((A ⊃ B) @ I) ⊃ ((A @ I) ⊃ (B @ I)))
2. ⊳ ((A @ I) ⊃ (B @ I)) ⊃ ((A ⊃ B) @ I)
Inference Rules: says as a $K$-Indexed Monad

\[
\frac{\psi; \Gamma \Rightarrow A[I]}{\psi; \Gamma \Rightarrow (K \text{ affirms } A) \text{ at } I} \quad \text{affirms}
\]

\[
\frac{\psi; \Gamma \Rightarrow (K \text{ affirms } A) \text{ at } I}{\psi; \Gamma \Rightarrow (K \text{ says } A)[I]} \quad \text{saysR}
\]

\[
\frac{\psi; \Gamma, (K \text{ says } A)[I], A[I] \Rightarrow (K \text{ affirms } B) \text{ at } I' \quad \psi \models I \supseteq I'}{\psi; \Gamma, (K \text{ says } A)[I] \Rightarrow (K \text{ affirms } B) \text{ at } I'} \quad \text{saysL}
\]

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. $\nvdash (K \text{ says } A) \supset A$
5. $\nvdash ((K \text{ says } A) @ I) \supset (K \text{ says } (A @ I))$
6. $\nvdash (K \text{ says } (A @ I)) \supset ((K \text{ says } A) @ I)$
Outline

1 Background
   ■ Motivating Example

2 $\eta$ Logic
   ■ Key Ideas and Judgments
   ■ Inference Rules and Admissible Properties
   ■ Meta-theory

3 Proof-Carrying Authorization (PCA) and Linearity

4 Conclusion
Meta-theory

Theorem (Admissibility of Cut)

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

- Entails the subformula property.
- Consequently, the connectives are defined \textit{entirely} by their left and right rules.

Theorem (Subsumption)

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

- Verifies desirable behavior of intervals.
- Verifies a proper fit between constraint and logical reasoning.
Principals state policies by digitally signing certificates.

When a principal requests access to a resource:

1. The certificates are converted to logical assumptions $\Gamma$; validity bounds $I$ are converted to $@I$ in $\Gamma$.

2. The principal must submit a proof of

$$\therefore \Gamma \implies A_{\text{access}}[\text{now, now} + \epsilon]$$

where:

- $A_{\text{access}}$ is the required formula to access the resource
- (By subsumption, it is sufficient to prove

$$\therefore \Gamma \implies A_{\text{access}}[I]$$

for any $I$ such that $\cdot \models I \supseteq [\text{now, now} + \epsilon]$.)

3. Access is granted if and only if the proof is correct.

Proof construction is now correct with respect to time.
Problem:

- As presented in this talk, $\eta$ logic cannot model consumable credentials.
- Alice probably wants Bob to enter \textit{at most once} during the week 6/23/08–6/30/08.

Solution:

- In our paper, $\eta$ 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

1 Background
   - Motivating Example

2 $\eta$ Logic
   - Key Ideas and Judgments
   - Inference Rules and Admissible Properties
   - Meta-theory

3 Proof-Carrying Authorization (PCA) and Linearity

4 Conclusion
Future Work and Summary

Future work:

- Formal comparison of $\eta$ logic to other logics and languages.
- Implementation of a PCA architecture based on $\eta$ logic.
- Extend non-interference theorems to $\eta$ 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 $\eta$ 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?
• 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.
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. \( (K \text{ affirms } A) \text{ at } I \): During \( I \), \( K \) affirms that *single-use* resource \( A \) is true on \( I \).

Refine hypothetical judgments:

1. \( \psi; \Gamma; \Delta \rightarrow A[I] \)
2. \( \psi; \Gamma; \Delta \rightarrow (K \text{ affirms } A) \text{ at } I \)

\[ \psi \models I \supseteq I' \]
\[ \frac{\psi; \Gamma; P[I] \rightarrow P[I']}{\psi; \Gamma; P[I'] \rightarrow P[I']} \text{ init} \]
\[ \psi; \Gamma, A[[I]]; \Delta, A[I] \rightarrow \gamma \]
\[ \frac{\psi; \Gamma, A[[I]]; \Delta \rightarrow \gamma}{\psi; \Gamma, A[[I]]; \Delta \rightarrow \gamma} \text{ copy} \]
Inference Rules: $\land$

$$\frac{\psi; \Gamma \Rightarrow A[\ell]}{\psi; \Gamma \Rightarrow (A \land B)[\ell]} \quad \land_R$$

$$\frac{\psi; \Gamma \Rightarrow B[\ell]}{\psi; \Gamma \Rightarrow (A \land B)[\ell]} \quad \land_R$$

$$\frac{\psi; \Gamma, (A \land B)[\ell], A[\ell] \Rightarrow \gamma}{\psi; \Gamma, (A \land B)[\ell] \Rightarrow \gamma} \quad \land L_1$$

$$\frac{\psi; \Gamma, (A \land B)[\ell], B[\ell] \Rightarrow \gamma}{\psi; \Gamma, (A \land B)[\ell] \Rightarrow \gamma} \quad \land L_2$$

1. $\vdash (A \land B) \equiv ((A \land B) \land (B \land B))$
Theorem (Identity)

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

- Generalizes the init rule to compound propositions.
Generic Non-Interference Theorem

- If $\psi; \Gamma, A[I] \rightarrow B[I']$ and $\langle$some criteria on $\psi, \Gamma, A, I, B, I'\rangle$, then $\psi; \Gamma \rightarrow B[I']$. 