Constructive Authorization Logics

Frank Pfenning

Carnegie Mellon University

Invited Talk

Workshop on Foundations of Computer Security (FCS'05)

Chicago, Illinois, June 30-July 1, 2005

Joint work with Deepak Garg and Kevin Watkins

Work in progress!

Outline

- Background
- Towards Universal Access Control
- Desiderata for Authorization
- Proof-Carrying Authorization
- Logic Design Principles
- Intuitionistic Authorization Logic
- Cut Elimination
- Independence and Non-Interference
- Most Closely Related Work
- Conclusion

Authentication and Authorization

- *Authentication*: who made a statement
  - Public key cryptography
  - Signed certificates
- *Authorization*: who should gain access to resource
  - Access control lists
  - Trust management
  - Relies on authentication

Authorization Logics

- *Authorization logics* provide a high-level, formal approach to access control in distributed systems
- Unifying basis for "*EEE*"
  - *Expressing* access control policy
  - *Enforcing* access control policy
  - *Exploring* consequences of access control policy
- Abstract away from
  - Mechanisms for authentication
  - Communication media and encryption
  - Protocols

Our Project

- *Distributed System Security via Logical Frameworks*
- PIs: Lujo Bauer, Mike Reiter, Frank Pfenning
- Supported by ONR N00014-04-1-0724 and NSF Cybertrust Center
- Using *smart phones* as “universal” access control device
  - Office door, computer (right now!)
  - Coffee machine? Car? Bank account? . . .

Sample Scenario

- Office door lock equipped with Bluetooth device
- Principal with smart phone approaches door
- Mutual discovery protocol
- Authorization dialog
- Door opens (or not)
- Implemented on CyLab floor, CiC, CMU

Sample Access Control Policy

- I can access my office
- The department head can access my office
- My secretary can access my office
- I trust my secretary to let others into my office
- My students can access my office
- The floor marshal can access my office
- I trust my wife in all things
- Anyone may ask me to get into my office

Desiderata for Authorization

- Expression, Enforcement, Exploration (EEE)
  - Expressive policy language
  - Simple enforcement of policies
  - Feasible reasoning about policies
- Extensibility
- Small trusted computing base
- Smooth integration of authentication
- Work with distributed information

Proof-Carrying Authorization

- Proof-carrying authorization
  [Appel & Felten'99] [Bauer'03]
- Express policy in authorization logic
- Prove right to access resource within logic
- Transmit actual proof object to resource
- Check proof object to grant access
- Authentication via signed statements
- First demonstration with web brower
  [Bauer, Schneider, Felten'02]

Scenario Revisited

- WeH 8117 is Frank's office
- WeH 8117 equipped with Bluetooth device
- Walk through two simple exchanges
- Illustrate basic ideas
- Ignoring discovery
- Ignoring freshness, nonces, etc.
- Handled in implementation

"I can open my office"

- Policy: *I can open my office*
- Frank approaches WeH 8117 with smart phone
- WeH 8117 challenges with

$$? : \mathsf{frank\ says\ open}(\mathsf{frank}, \mathsf{weh.8117})$$

- Policy embodied in challenge
- Frank signs

$$\mathsf{frank\ says\ open}(\mathsf{frank}, \mathsf{weh.8117})$$

to obtain $\mathsf{c38d9103294}$

"I can open my office"

- Frank replies

$$\mathsf{x509(c38d9103294)}$$

- WeH 8117 checks (trivial) proof

$$\mathsf{x509(c38d9103294) : frank\ says\ open(frank, weh.8117)}$$

- Door opens
- Proof checking requires certificate checking for authentication

"My secretary can open my office"

- Policy: *My secretary can open my office*
- Policy expressed as policy axiom

$$
\begin{aligned}
\mathsf{r1} : \mathsf{frank}\ \mathsf{says}\ & \\
& \forall S.\ \mathsf{depthead}\ \mathsf{says}\ \mathsf{secretary}(\mathsf{frank}, S) \\
& \quad \supset \mathsf{frank}\ \mathsf{says}\ \mathsf{open}(S, \mathsf{weh.8117})
\end{aligned}
$$

- Policy known to Jenn, Frank, and WeH 8117
- Jenn approaches WeH 8117 with smart phone
- WeH 8117 challenges with

$$\mathsf{frank}\ \mathsf{says}\ \mathsf{open}(\mathsf{jenn}, \mathsf{weh.8117})$$

"My secretary can open my office"

- Jenn asks database (silent phone call)

$$? : \mathsf{depthead\ says\ secretary}(\mathsf{frank}, \mathsf{jenn})$$

- Database replies with signed certificate as proof

$$\mathsf{x509}(\mathsf{cdksi92899}) : \mathsf{depthead\ says\ secretary}(\mathsf{frank}, \mathsf{jenn})$$

- Jenn assembles and sends proof

$$\mathsf{r1}(\mathsf{x509}(\mathsf{cdksi92899}))$$

- WeH 8117 checks

$$\mathsf{r1}(\mathsf{x509}(\mathsf{cdksi92899})) : \mathsf{frank\ says\ open}(\mathsf{jenn}, \mathsf{weh.8117})$$

- Door opens

"My secretary can open my office"

- Could also relativize "my office"

$$\forall P. \forall O. \textsf{depthead says office}(P, O) \supset \textsf{office}(P, O)$$

$$\forall P. \forall O. \textsf{office}(P, O) \supset \textsf{open}(P, O)$$

- Simplified proof expression here for brevity
- Knowledge can be shared and distributed since signed
- Certificates and proofs can be cached
- Checking certificates checks expiration

Authorization Logic Implementation

- Representation in Logical Framework
  - Logic: LF signature
  - Policy: LF signature of restricted form
  - Proof: LF object
- Proof generation [Bauer, Garriss, Reiter'05]
  - Extensive caching to minimize communication
  - Distributed certifying prover
- Proof checking
  - X.509 certificate checking
  - Proof checking as LF type checking

Some Authorization Logic Issues

- Intuitionistic or classical?
- Laws for "says" modality?
- Set of logical connectives?
- Propositional or first-order or higher-order?
- Decidable?
- Monotonic?
- Temporal?

Logic Design Principles

- Proof-theoretic semantics
  [Martin-Löf'83] [Pf & Davies'01]
  - Separating judgments from propositions
  - Characterize connectives and modalities via their rules
  - Cut elimination and identity principles
  - Focusing [Andreoli'92]
- Consequences
  - Independence of logical connectives from each other
  - Intuitive interpretation
  - Amenable to meta-theoretic analysis (exploration!)
  - Open-ended design (extensibility!)

Judgments

- *Judgments* are objects of knowledge
- *Evidence* for judgments is given by deductions
- Basic judgments
  - $A\ true$ — proposition A is true
  - $P\ \mathit{aff}\ A$ — principal P affirms proposition A
- Logical connectives are defined by their *introduction* and *elimination* rules
- Must match in certain ways to be meaningful
- Here, truth is almost subsidiary, because affirmation expresses intent

Hypothetical Judgments

- *Hypothetical judgments* for reasoning from assumptions

$$J_1, \ldots, J_n \vdash J$$

- Will freely reorder assumptions
- *Hypothesis rule*

$$\frac{}{\Gamma, J \vdash J}$$

- *Substitution principle*

If $\quad \Gamma \vdash J \quad$ *and* $\quad \Gamma, J \vdash J' \quad$ *then* $\quad \Gamma \vdash J'$.

- Fixes meaning of hypothetical judgments

Implication

- Introduction rule

$$\frac{\Gamma, A\ \mathit{true} \vdash B\ \mathit{true}}{\Gamma \vdash A \supset B\ \mathit{true}} \supset I$$

- Elimination rule

$$\frac{\Gamma \vdash A \supset B\ \mathit{true} \quad \Gamma \vdash A\ \mathit{true}}{\Gamma \vdash B\ \mathit{true}} \supset E$$

Local Soundness

- An introduction followed by any elimination of a connective can be reduced away
- Shows elimination rules are not too strong

$$\dfrac{\dfrac{\begin{array}{c}\mathcal{E}\\ \Gamma, A\ \mathit{true} \vdash B\ \mathit{true}\end{array}}{\Gamma \vdash A \supset B\ \mathit{true}}\supset I \qquad \begin{array}{c}\mathcal{D}\\ \Gamma \vdash A\ \mathit{true}\end{array}}{\Gamma \vdash B\ \mathit{true}}\supset E \quad \Longrightarrow_R \quad \begin{array}{c}\mathcal{E}'\\ \Gamma \vdash B\ \mathit{true}\end{array}$$

- $\mathcal{E}'$ constructed by substituting $\mathcal{D}$ in $\mathcal{E}$
- Possible by substitution principle

Local Completeness

- There is a way to apply eliminations to a compound proposition so we can reintroduce the proposition from the results
- Shows elimination rules are not too weak

$$\begin{array}{c}\mathcal{D} \\ \Gamma \vdash A \supset B \; true\end{array} \quad \Longrightarrow_E \quad \dfrac{\dfrac{\begin{array}{c}\mathcal{D}' \\ \Gamma, A\; true \vdash A \supset B \; true\end{array} \quad \overline{\Gamma, A\; true \vdash A \; true}}{\Gamma, A\; true \vdash B \; true} \supset E}{\Gamma \vdash A \supset B \; true} \supset I$$

- $\mathcal{D}'$ constructed by weakening from $\mathcal{D}$

Truth and Affirmation

- Define *affirmation judgment* relative to truth
- If A is true then any P affirms A

$$\frac{\Gamma \vdash A\ \mathit{true}}{\Gamma \vdash P\ \mathit{aff}\ A}$$

- If P affirms A, then we can assume A is true, but only while establishing an affirmation by P

  If $\quad \Gamma \vdash P\ \mathit{aff}\ A \quad$ *and* $\quad \Gamma, A\ \mathit{true} \vdash P\ \mathit{aff}\ C$
  then $\quad \Gamma \vdash P\ \mathit{aff}\ C$

Internalizing Judgments

- Implication internalizes hypothetical reasoning
- "says" modality internalizes affirmation
- Introduction rule

$$\frac{\Gamma \vdash P \ \mathit{aff} \ \ A}{\Gamma \vdash (P \ \textsf{says} \ A) \ \ \mathit{true}} \ \textsf{says}I$$

- Elimination rule

$$\frac{\Gamma \vdash (P \ \textsf{says} \ A) \ \ \mathit{true} \qquad \Gamma, A \ \mathit{true} \vdash P \ \mathit{aff} \ \ C}{\Gamma \vdash P \ \mathit{aff} \ \ C} \ \textsf{says}E$$

Local Soundness

- Reduce introduction followed by elimination

$$\dfrac{\dfrac{\begin{array}{c}\mathcal{D}\\ \Gamma \vdash P\ \mathit{aff}\ A\end{array}}{\Gamma \vdash (P\ \mathsf{says}\ A)\ \mathit{true}}\ \mathsf{says}I \qquad \begin{array}{c}\mathcal{E}\\ \Gamma, A\ \mathit{true} \vdash P\ \mathit{aff}\ C\end{array}}{\Gamma \vdash P\ \mathit{aff}\ C}\ \mathsf{says}E$$

$$\Longrightarrow_R \quad \begin{array}{c}\mathcal{E}'\\ \Gamma \vdash P\ \mathit{aff}\ C\end{array}$$

- $\mathcal{E}'$ is constructed from $\mathcal{D}$ and $\mathcal{E}$
- Exists by definition of affirmation

Local Completeness

- Eliminate to re-introduce

$$\begin{array}{c}\mathcal{D}\\ \Gamma \vdash (P \;\textsf{says}\; A)\ \mathit{true}\end{array} \quad \Longrightarrow_E$$

$$\dfrac{\dfrac{\begin{array}{c}\mathcal{D}\\ \Gamma \vdash (P \;\textsf{says}\; A)\ \mathit{true}\end{array} \quad \dfrac{\overline{\Gamma, A\ \mathit{true} \vdash A\ \mathit{true}}}{\Gamma, A\ \mathit{true} \vdash P\ \mathit{aff}\ A}}{\Gamma \vdash P\ \mathit{aff}\ A}\,\textsf{says}E}{\Gamma \vdash (P \;\textsf{says}\; A)\ \mathit{true}}\,\textsf{says}I$$

Some Consequences

- Principals are isolated: they only share truth!
- Dependencies only from policy axioms

$$\begin{array}{l} \mathsf{frank\ says} \\ \quad \forall S.\ \mathsf{depthead\ says\ secretary}(\mathsf{frank}, S) \\ \qquad \supset \mathsf{frank\ says\ open}(S, \mathsf{weh.8117}) \end{array}$$

Affirmation as Indexed Monad

- P-indexed family of strong monads
  - $\vdash A \supset (P \text{ says } A)$
  - $\vdash (P \text{ says } A) \supset (A \supset (P \text{ says } C)) \supset (P \text{ says } C)$
  - $\vdash (A \supset B) \supset ((P \text{ says } A) \supset (P \text{ says } B))$
  - $\vdash (P \text{ says } (P \text{ says } A)) \supset (P \text{ says } A)$
- Strong monads used in functional programming to isolate effects
- $P \text{ says } A$ corresponds to $\bigcirc A$ from *lax logic* [Benton, Bierman, de Paiva'98]
- Decomposes into $\Diamond\Box A$ from *modal logic* CS4 [Pf. & Davies'01]

Other Connectives

- Judgmental foundation allows *modular* addition of new connectives by introductions and eliminations
- Quantifiers are also straightforward
- Some consequences:
  - $\vdash ((P \text{ says } A) \vee (P \text{ says } B)) \supset (P \text{ says } (A \vee B))$
  - $\not\vdash (P \text{ says } (A \vee B)) \supset ((P \text{ says } A) \vee (P \text{ says } B))$
  - $\vdash \bot \supset (P \text{ says } \bot)$
  - $\not\vdash (P \text{ says } \bot) \supset \bot$
- Last property is critical, since principals are not constrained in what they affirm

Cut Elimination

- How do we prove $\not\vdash (P \text{ says } \bot) \supset \bot$?
- Generalize from local soundness and local completeness to global properties
- Via cut-free atomic sequent calculus
- Show cut and identity principle are admissible

Sequent Calculus

- Introduce new basic judgment $A\ hyp$ — proposition A is hypothesis
- Use only on left-hand side of hypothetical
  - $A_1\ hyp, \ldots, A_n\ hyp \vdash A\ true$ (write: $\Delta \Rightarrow A\ true$)
  - $A_1\ hyp, \ldots, A_n\ hyp \vdash P\ \mathit{aff}\ A$ (write: $\Delta \Rightarrow P\ \mathit{aff}\ A$)
- Judgmental rules

$$\frac{(a \text{ atomic})}{\Delta, a\ hyp \Rightarrow a\ true} \qquad \frac{\Delta \Rightarrow A\ true}{\Delta \Rightarrow P\ \mathit{aff}\ A}$$

Sequent Rules

- Right rule from intro, left rule from elim
- Omit (implicit) contraction
- J either C *true* or P *aff* C

$$\frac{\Delta, A\ hyp \Rightarrow B\ true}{\Delta \Rightarrow A \supset B\ true}\supset R \qquad \frac{\begin{array}{c}\Delta \Rightarrow A\ true \\ \Delta, B\ hyp \Rightarrow J\end{array}}{\Delta, A \supset B\ hyp \Rightarrow J}\supset L$$

$$\frac{\Delta \Rightarrow P\ aff\ A}{\Delta \Rightarrow (P\ \textsf{says}\ A)\ true}\textsf{says}R \qquad \frac{\Delta, A\ hyp \Rightarrow P\ aff\ C}{\Delta, (P\ \textsf{says}\ A)\ hyp \Rightarrow P\ aff\ C}\textsf{says}L$$

Cut and Identity

- Cut (global soundness)

  If $\Delta \Rightarrow A\,\mathit{true}$ *and* $\Delta, A\,\mathit{hyp} \Rightarrow J$ *then* $\Delta \Rightarrow J$

- Proof by simple nested structural induction on A and the two given derivations
- Identity (global completeness)

  $\Delta, A\,\mathit{hyp} \Rightarrow A\,\mathit{true}$ for any proposition A

- Proof by simple structural induction on A
- $\Gamma \vdash J$ iff $\Gamma \Rightarrow J$ (from cut, with abuse of notation)

Some Easy Consequences

- Subformula property
- Immediate independence results
  - $\not\Rightarrow \bot\ \mathit{true}$
  - $\not\Rightarrow P\ \mathit{aff}\ \bot$
  - $(P\ \textsf{says}\ \bot)\ \mathit{hyp} \not\Rightarrow \bot\ \mathit{true}$
  - $A \supset (P\ \textsf{says}\ B)\ \mathit{hyp} \not\Rightarrow (P\ \textsf{says}\ (A \supset B))\ \mathit{true}$
- Simple non-interference

  If Δ and J do not mention P, then
  $\Delta, P\ \textsf{says}\ A_1\ \mathit{hyp}, \ldots, P\ \textsf{says}\ A_n\ \mathit{hyp} \Rightarrow J$ *iff*
  $\Delta \Rightarrow J$*.*

Reasoning About Logic and Policies

- We have formally verified cut in Twelf (proof explicitly supplied) [Pf & Schürmann'99, Pf'00, Garg'05]
- Some independence results are easily verified formally
- Conjecture: these can be proven automatically [Pf & Schürmann'98]
- Deeper reasoning about policies (= sets of axioms) is tricky
  - Requires (at least) focusing
  - Clean proof theory may enable some results

Expressive Power

- Easy
  - Groups and roles
  - Delegation of specific rights
  - Joint authorization
- Slightly more complicated (not yet verified)
  - Full delegation
  - Creating new principals

Intuitionistic vs Classical Logic

- Intuitionistic logic as logic of explicit evidence
- Sample classical, but not intuitionistic truth [Abadi'03]

$$(P \text{ says } A) \supset (A \vee (P \text{ says } B)) \quad \text{for any } B$$

- Classical logic is *descriptive*, arises from structure
- Intuitionistic logic is *creative*, arises from properties
- Authorization is not given explicitly by a structure, but by properties (non-interference)

Authorization Logic Issues, Revisited

- Intuitionistic or classical? (intuitionistic)
- Laws for says modality? (indexed family of strong monads)
- Set of logical connectives? (open-ended)
- Propositional or first-order or higher-order? (first-order)
- Decidable? (no, fragment tractable?)
- Monotonic? (yes)
- Temporal? (no)

Monotonicity

- Nonmononticity dubious in distributed setting
- Instead, for access revocation:
  - Short-lived certificates
  - $\mathsf{notRevoked}$ predicate
  - External reasoning about time
- Ephemeral capabilities (future work)
  - Digital rights managment
  - Electronic payment
  - Bounded delegation
  - Via *linear connectives in authorization logic*?

Most Closely Related Work

- [Abadi, Burrows, Lampson, Plotkin'93]
  propositional, axiomatic, rich calculus of principals
- [Appel & Felten'99] [Bauer'03] (PCA)
  classical, higher-order, no analysis of modalities
- [De Treville'02] (Binder)
  datalog, decidable, modality not classified
- [Rueß & Shankar'03] (Cyberlogic)
  intuitionistic, unjustified modal laws, semi-axiomatic style, more ambitious scope (protocols), proof-carrying
- [Abadi, LICS 2003] structured overview, further references

Desiderata Revisited

- Expression, Enforcement, Exploration (EEE)
  - Expressive policy language
  - Simple enforcement of policies
  - Feasible reasoning about policies
- Extensibility
- Small trusted computing base
- Smooth integration of authentication
- Work with distributed information

Conclusion

- Design of authorization logic as modal logic
  - Judgmental, constructive, open-ended, modular
  - Affirmation as indexed strong monad
  - Basic cut elimination formally verified
- Next
  - Extend verification to more connectives
  - Stronger non-interference properties
  - Cell-phone implementation (currently higher-order logic)
- Eventually:
  - Linear authorization logic for ephemeral capabilities (digital rights, electronic payments, bounded delegation)?