

# Proof-Carrying Authorization

Ruy Ley-Wild

Computer Science Department  
Carnegie Mellon University

September 26, 2007

# Proof-Carrying Authorization

- ▶ Proof-Carrying Authentication  
A. W. Appel and E. W. Felten  
Computer and Communications Security 1999
- ▶ Access Control for the Web via Proof-Carrying Authorization  
L. Bauer  
PhD Thesis 2003
- ▶ ~~Consumable Credentials in Logic-Based Access Control  
L. Bauer, K. D. Bowers, F. Pfenning, M. K. Reiter  
Network and Distributed System Security Symposium 2007~~

# Motivation

- ▶ Incompatible authentication/authorization mechanisms
  - ▶ Features of one system may not be expressible in another
  - ▶ Poor interoperability due to cross-realm trust
  - ▶ Hard or impossible to cross-authenticate/authorize
- ▶ Gap between logical formalisms and implementations

# Goals

- ▶ Interoperability and expressiveness
  - ▶ Facts may be collected from multiple servers
  - ▶ Don't rely on policy/mechanism compatibility
- ▶ Generality
  - ▶ Multiple authorization logics may be encoded in framework
  - ▶ Independent of resource being protected
  - ▶ Decouple authentication and authorization
    - ▶ Authorization need not depend on identification
- ▶ Ease of use
  - ▶ Transparent access to user (after initial setup)
- ▶ Efficiency

# Proof-Carrying Authorization

- ▶ Logical framework encodes multiple authorization mechanisms
- ▶ Shift burden of proof of authorization from server to client
  - ▶ Server
    - ▶ powerful logical framework for interoperability
    - ▶ issues challenge theorem
    - ▶ checks proof of authorization in logical framework
  - ▶ Client
    - ▶ weak application-specific logic per authorization mechanism
    - ▶ collects valid hypotheses from fact servers
    - ▶ constructs proof of authorization in application-specific logic
    - ▶ submits preferred ASL encoding and proof of authorization
- ▶ Decouple authentication and authorization
- ▶ Tighten connection between theory and implementation

- Alice wants to access `http://server/midterm.html`
- Alice knows it's after 8 P.M.

Alice  
(web browser)



Bob  
(web server)



- Bob publishes `midterm.html` on the web
- He wants the page to be visible only by students in CS101 and only after 8 P.M.

Registrar  
(fact server)

- The Registrar knows that Alice is taking CS101



# Two Logics

- ▶ General logical framework for distributed authorization
  - ▶ Undecidable higher-order logic
  - ▶ Server only needs to check decidable proofs
  - ▶ Independent of policies and resources
- ▶ Simple application-specific logic per authorization mechanism
  - ▶ Client free to choose (decidable) application-specific logic(s)
  - ▶ Client must collect enough hypotheses and construct proof
  - ▶ Interpret ASL in HOL

# ASL Syntax

- ▶ Variant of ABLP logic

$N \in \mathbb{N}$

$S \in \mathbf{String}$

$P ::= \mathbf{name}(S) \mid \mathbf{name}(S).S$  principal

$F ::= S \mathbf{signed} \psi \mid P \mathbf{says} \psi$  formula

$\psi ::= \mathbf{goal}(S, S) \mid \delta \mathbf{before} N \mid \delta \mathbf{after} N \mid \delta$  statement

$\delta ::= P \mathbf{speaksfor} P \mid \mathbf{delegate}(P, P, S)$  delegation

$\Gamma ::= \cdot \mid \Gamma, S \mathbf{signed} \psi$  context

# ASL Syntax (Revised)

$N \in \mathbb{N}$

$S \in \mathbf{String}$

$U \in \mathbf{URL}$

$K \in \mathbf{Key}$

$P ::= \mathbf{name}(K) \mid \mathbf{name}(K).S$

principal

$F ::= K \mathbf{signed} F \mid P \mathbf{says} F \mid F \mathbf{before} N \mid F \mathbf{after} N \mid \psi$

formula

$\psi ::= \mathbf{goal}(U, N) \mid P \mathbf{speaksfor} P \mid \mathbf{delegate}(P, P, U)$

statement

$\Gamma ::= \cdot \mid \Gamma, K \mathbf{signed} \psi$

context

# ASL Rules

- ▶ Judgment  $\Gamma \vdash F$
- ▶ Server grants access to  $U$  in session  $N$  if client can prove

$$\Gamma \vdash \text{Server } \mathbf{says\ goal}(U, N)$$

- ▶ Context  $\Gamma$  is invariant throughout proofs
- ▶ Constants defined extralogically or by proof rules

# ASL Extralogical Constants

- ▶ Extralogical Constants
  - ▶ **name**( $K$ ) means the principal with public key  $K$
  - ▶ **name**( $K$ ). $S$  means **name**( $K$ )'s local name  $S$
  - ▶  $K$  **signed**  $\psi$  embodies extralogical digital signatures
  - ▶ **goal**( $U, N$ ) means the desired resource is url  $U$  in session  $N$
- ▶ Proof-checking requires external mechanism for verification

# ASL Rules for Belief

- ▶  $A$  **says**  $\psi$  means  $A$  believes  $\psi$

$$\frac{\text{pubkey } \mathbf{signed} \ \psi}{\mathbf{name(pubkey) says} \ \psi} \text{SAYSI}$$

## ASL Rules for Specific Delegation

- ▶ **delegate**( $A, B, U$ ) means  $B$  may access  $U$  on  $A$ 's behalf

$$\frac{A \text{ says } \mathbf{delegate}(A, B, U) \quad B \text{ says } \mathbf{goal}(U, N)}{A \text{ says } \mathbf{goal}(U, N)} \text{ DELEGATEE}$$

$$\frac{A \text{ says } \mathbf{delegate}(A, B.S, U) \quad B.S \text{ says } \mathbf{goal}(U, N)}{A \text{ says } \mathbf{goal}(U, N)} \text{ DELEGATEE2}$$

## ASL Rules for General delegation

- ▶  $A$  **speaksfor**  $B$  means  $A$  may speak on  $B$ 's behalf

$$\frac{A \text{ says } B \text{ speaksfor } A \quad B \text{ says goal}(U, N)}{A \text{ says goal}(U, N)} \text{ SPEAKSFOR E}$$

$$\frac{A \text{ says } B \text{ speaksfor } A.S \quad B \text{ says goal}(U, N)}{A.S \text{ says goal}(U, N)} \text{ SPEAKSFOR E2}$$

- ▶ Tantamount to **delegate**( $B, A, U$ ) for every  $U$

# ASL Rules for Temporal Restriction

- ▶  $\psi$  **before**  $N$  means  $\psi$  holds before time  $N$   
 $\psi$  **after**  $N$  means  $\psi$  holds after time  $N$

$$\frac{A \text{ says } (\psi \text{ before } N) \quad (time < N)}{A \text{ says } \psi} \text{ BEFOREE}$$

$$\frac{A \text{ says } (\psi \text{ after } N) \quad (time > N)}{A \text{ says } \psi} \text{ AFTERE}$$

- ▶ Informal side condition on time

# ASL Rules

$$\frac{\text{pubkey signed } \psi}{\text{name(pubkey) says } \psi} \text{ SAYS I}$$

$$\frac{A \text{ says delegate}(A, B, U) \quad B \text{ says goal}(U, N)}{A \text{ says goal}(U, N)} \text{ DELEGATE E}$$

$$\frac{A \text{ says } B \text{ speaksfor } A \quad B \text{ says goal}(U, N)}{A \text{ says goal}(U, N)} \text{ SPEAKSFORE}$$

$$\frac{A \text{ says } (\psi \text{ before } N) \quad (time < N)}{A \text{ says } \psi} \text{ BEFORE E}$$

$$\frac{A \text{ says } (\psi \text{ after } N) \quad (time > N)}{A \text{ says } \psi} \text{ AFTER E}$$

# ASL Decidability

- ▶ Interpret as graph reachability
  - ▶ Discard unusable/irrelevant facts
  - ▶ One node per principal
  - ▶ One directed edge according to delegation
  - ▶ Find directed path between client and server
- ▶ Interpret as bottom-up logic program
  - ▶ ASL inference rules and initial context as clauses
  - ▶ Query *Server* **says goal**( $U, N$ )

# ASL Local Soundness

- ▶ Cannot mistakenly conclude access to resource

$A$  **says goal**( $U, N$ )

- ▶ Structural analysis of rules

- ▶  $pubkey_A$  **signed goal**( $U, N$ ) cannot be forged

$$\frac{pubkey \text{ signed } \psi}{name(pubkey) \text{ says } \psi} \text{ SAYS I}$$

- ▶  $A$  **says delegate**( $A, B, U$ ) by explicit delegation and  $B$  **says goal**( $U, N$ ) (inductively) cannot be forged

$$\frac{A \text{ says delegate}(A, B, U) \quad B \text{ says goal}(U, N)}{A \text{ says goal}(U, N)} \text{ DELEGATE E}$$

- ▶ ...

# PCA Logical Framework

- ▶ Higher-order logic
  - ▶ Powerful enough to describe many application-specific logics
    - ▶ Only one example ASL
  - ▶ More general and concise than  $k^{\text{th}}$ -order logic
    - ▶ ASL may be too restricted to exploit advantages of HOL
  - ▶ Can encode modal and linear notions
    - ▶ Perhaps preferable to have as primitive notions
- ▶ PCA is HOL with constants for authorization

# PCA (HOL) Rules

$$\frac{[F] \quad G}{F \supset G} \supset I$$

$$\frac{F \quad F \supset G}{G} \supset E$$

$$\frac{[Y/x]F}{\forall x.F} \forall I$$

$$\frac{\forall x.F}{[Y/x]F} \forall E$$

$$\frac{F}{(\lambda x.[x/Y]F)Y} \beta I$$

$$\frac{(\lambda x.F)Y}{[Y/x]F} \beta E$$

$$\frac{}{F(X_i) \supset F(\pi_i \langle X_1, X_2 \rangle)} \pi$$

$$\frac{}{\neg\neg F \supset F} \neg\neg E$$

## PCA (HOL) Abbreviations

$$F = G \triangleq \forall P. P(F) \supset P(G)$$

$$F \wedge G \triangleq \forall H. (F \supset G \supset H) \supset H$$

$$F \vee G \triangleq \forall H. (F \supset H) \supset (G \supset H) \supset H$$

$$\exists P \triangleq \forall F. (\forall G. P(G) \supset F) \supset F$$

$$\perp \triangleq \forall F. F$$

$$\neg F \triangleq F \supset \perp$$

# PCA: Encoding ASL

- ▶ Uninterpreted HOL constants

**worldview** = **string**

**name** : **string** → **worldview**

**goal** : **string** → **string** → **formula**

**signed** : **string** → **formula** → **formula**

**localtime** : **nat**

- ▶ Semantics of constants left to ASL designer

## PCA: ASL Interpretation

- ▶ Define interpretation of ASL in HOL
  - ▶ Give HOL rules mimicking ASL rules
  - ▶ Give HOL definition of ASL constants
  - ▶ Show rules are admissible according to definition
- ▶ Belief as guiding principle
- ▶ Rational and accountable principals

## PCA: ASL Interpretation of Belief

- ▶ A principal's beliefs should be internally and externally consistent
  - ▶ not part of ASL

$$\frac{F}{A \text{ says } F} \text{ TAUT}$$

$$\frac{A \text{ says } F \quad A \text{ says } F \supset G}{A \text{ says } G} \text{ MP}$$

- ▶ Internalize ASL's SAYSI

$$\frac{K \text{ signed } F}{\text{name}(K) \text{ says } F} \text{ SAYSI}$$

# PCA: ASL Interpretation of Belief

- ▶ Define **says** as HOL relation

$$A \text{ says } F \triangleq \forall P. \left[ \begin{array}{l} \forall B. \forall G. \forall H. \forall K. \\ G \supset P(B, G) \\ \wedge P(B, G) \supset P(B, G \supset H) \supset P(B, H) \\ \wedge K \text{ signed } G \supset P(\text{name}(K), G) \end{array} \right] \supset P(A, F)$$

- ▶ TAUT, MP, SAYS I rules are admissible
  - ▶ if the premises hold then so does the conclusion
  - ▶ using definition of **says**
- ▶ Other rules are admissible

$$\frac{A \text{ says } A \text{ says } F}{A \text{ says } F} \text{IDEM}$$

## PCA: ASL Interpretation of Local Names

- ▶ Derived form for local names
- ▶ Additional interpretation for every constant involving names

$$A.S \text{ says } F \triangleq A \text{ says name}(S) \text{ says } F$$

- ▶ Not uniform: local names aren't terms in their own right

## PCA: ASL Interpretation of Specific Delegation

- ▶ **delegate**( $A, B, U$ ) means Bob's beliefs about  $U$  imply Alice's

$$\mathbf{delegate}(A, B, U) \triangleq \forall N. B \mathbf{says goal}(U, N) \supset A \mathbf{says goal}(U, N)$$

- ▶ DELEGATEE rule is admissible
- ▶ Doesn't show invalid delegation is inadmissible

$$\frac{A \mathbf{says delegate}(C, B, U) \quad B \mathbf{says goal}(U, N)}{C \mathbf{says goal}(U, N)} \text{ DELEGATEE'}$$

# PCA: ASL Interpretation of General Delegation

- ▶  $A$  **speaksfor**  $B$  means Bob's beliefs imply Alice's

$$A \text{ **speaksfor** } B \triangleq \forall U. \text{**delegate**}(B, A, U)$$

- ▶ SPEAKSFOR $\bar{E}$  rule is admissible
- ▶ Doesn't show invalid delegation is inadmissible

$$\frac{A \text{ **says** } B \text{ **speaksfor** } C \quad B \text{ **says** } \text{goal}(U, N)}{C \text{ **says** } \text{goal}(U, N)} \text{SPEAKSFOR}\bar{E}'$$

# PCA: ASL Interpretation of Time

- ▶ **localtime** represents current time on local host
- ▶  $F$  **before**  $N$  means belief in  $F$  is contingent on  $N$  in the future
- ▶  $F$  **after**  $N$  means belief in  $F$  is contingent on  $N$  in the past

$$F \text{ before } N \triangleq \text{localtime} < N \supset F$$

$$F \text{ after } N \triangleq \text{localtime} > N \supset F$$

- ▶ BEFORE<sub>E</sub> and AFTER<sub>E</sub> rules are admissible

$$\frac{A \text{ says } (F \text{ before } N) \quad \text{localtime} < N}{A \text{ says } F} \text{ BEFORE}_E$$

$$\frac{A \text{ says } (F \text{ after } N) \quad \text{localtime} > N}{A \text{ says } F} \text{ AFTER}_E$$

## ASL Extension: Principal Hierarchy

- ▶ Generalize principals to arbitrary local names

**name**( $K$ ). $\vec{S}$

- ▶ Generalize connectives

**name**( $K$ ). $S_1 \dots S_n$  **says'**  $F = \mathbf{name}(K)$  **says**  $S_1$  **says**  $\dots S_n$  **says**  $F$

# ASL Extension: Certification Authority and Revocation

- ▶ CA has local name for principal, binds key

*CA **signed name**( $pubkey_{Alice}$ ) **speaksfor** CA.Alice*

- ▶ CA may impose expiration

*CA **signed** (**name**( $pubkey_{Alice}$ ) **speaksfor** CA.Alice **before** expiration)*

# ASL Extension: Certification Authority and Revocation

- ▶ Nonmonotonic revocation
  - ▶ Revocation list forces deletion of existing certificates
- ▶ Monotonic revocation
  - ▶ Certificates depend on valid revocation list
  - ▶ **cert**( $A, F, N$ ) means  $A$  believes  $F$ , certificate numbered  $N$

$$\mathbf{cert}(A, F, N) \triangleq A \mathbf{signed\ name}(serial) \mathbf{says\ name}(N) \mathbf{says} F$$

- ▶ **revlist**( $T_1, T_2, L$ ) revokes certificates  $L$  during  $]T_1, T_2]$

$$\mathbf{revlist}(T_1, T_2, L) \triangleq \forall N. \forall F.$$

$$T_1 < \mathbf{localtime} \leq T_2$$

$$\supset N \notin L$$

$$\supset \mathbf{name}(serial) \mathbf{says\ name}(N) \mathbf{says} F$$

$$\supset F$$

$$\mathbf{cert}(A, F, N)$$

$$A \mathbf{signed\ revlist}(T_1, T_2, L) \quad T_1 < \mathbf{localtime} \leq T_2 \quad N \notin L$$

---

$$A \mathbf{says} F$$

## PCA: Semantic Soundness

- ▶ Cannot mistakenly derive  $\perp$
- ▶ All constants are interpreted as HOL formulas
  - ▶ Interpret  $A$  **signed**  $F$  as  $\lambda A.\lambda F.\top$
  - ▶ But maybe can derive  $A$  **says**  $\perp$
- ▶ HOL is consistent
- ▶ Therefore PCA with ASL interpretation is consistent

# Cons

- ▶ Lacks justification of application-specific logic
- ▶ Semantic soundness doesn't prevent flawed interpretation
- ▶ HOL may be too powerful as logical framework
- ▶ No mechanism for bootstrapping authentication
- ▶ Server can't be completely oblivious to ASL
- ▶ May still be difficult to compose ASL's

# Pros

- ▶ Decouple authorization from authentication
- ▶ Decouple authorization mechanism from framework
- ▶ Decouple proof construction and proof verification
- ▶ Interpret constants according to proof rules
- ▶ Use logic to reason about and implement authorization policy