CS 5430:

Formal Analysis of a Hierarchical Certification Authority

Fred B. Schneider

Samuel B Eckert Professor of Computer Science

Department of Computer Science
Cornell University
Ithaca, New York 14853
U.S.A.

Cornell CIS
Computer Science

CAL

Language:

$$
\begin{array}{lll}
C ::= & F & \text{(F } \textit{a formula of First-order Predicate Logic}\text{)} \\
 & | & P\ \textbf{says}\ C \\
 & | & P'\ \textbf{speaksfor}\ P \\
 & | & P'\ \textbf{speaks}\ x{:}C\ \textbf{for}\ P \\
 & | & C \wedge C' \\
 & | & C \vee C' \\
 & | & C \Rightarrow C'
\end{array}
$$

N.b. $\neg C$: $(C \Rightarrow \text{false})$

Models for CAL

ω(P) is the set of beliefs principal P has.

- P **says** C iff $C \in \omega(P)$
- P' **speaksfor** P iff $\omega(P') \subseteq \omega(P)$

ω(P) called the **worldview** of P

CAL Inference Rules: **says**

$$\frac{C}{P\ \textbf{says}\ C}\qquad\qquad \frac{P\ \textbf{says}\ C}{P\ \textbf{says}\ (\,P\ \textbf{says}\ C\,)}\qquad\qquad \frac{P\ \textbf{says}\ (\,P\ \textbf{says}\ C\,)}{P\ \text{says}\ C}$$

$$\frac{P\ \textbf{says}\ (C \Rightarrow C')}{(P\ \textbf{says}\ C\,) \Rightarrow\ (\,P\ \textbf{says}\ C')}$$

Example CAL Proof (1)

$$P\ \textbf{says}\ C, \qquad P\ \textbf{says}\ (\ C \Rightarrow C'\ )$$

Example CAL Proof (2)

$$P \textbf{ says } C, \quad \frac{P \textbf{ says } (\, C \Rightarrow C'\,)}{(P \textbf{ says } C) \Rightarrow (P \textbf{ says } C')}$$

Example CAL Proof (3)

$$\frac{P \textbf{ says } C, \quad \dfrac{P \textbf{ says } (\, C \Rightarrow C')}{(P \textbf{ says } C) \Rightarrow (P \textbf{ says } C')}}{P \textbf{ says } C'}$$

CAL Inference Rules: speaksfor

$$\frac{P \textbf{ says } (P' \textbf{speaksfor } P)}{P' \textbf{speaksfor } P} \text{ hand-off}$$

$$\frac{P' \textbf{speaksfor } P}{(P' \textbf{says } C) \Rightarrow (P \textbf{ says } C)}$$

$$\frac{P \textbf{ speaksfor } P', P' \textbf{speaksfor } P''}{P \; \boldsymbol{speaksfor} \; P''}$$

Credentials Can Convey Beliefs

k_S is a signing key; K_S is a verification key

k_S-**sign**(C): K_S **says** C

- Public keys are principals.
- K_S **speaksfor** S if principal S is the only agent with access to private key k_S.

A principal S can be a hash of the running code and data that was read.

Application

Public Key Infrastructure (PKI)

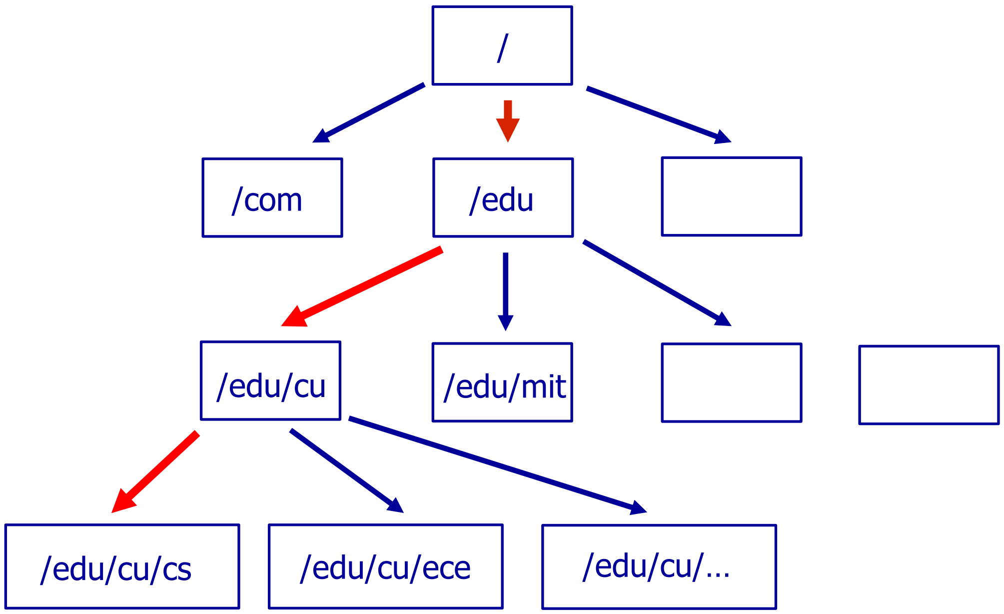
k_S-**sign**(C):

- Certificate: K_S-$\langle C \rangle$
- CAL formalization: K_S **says** C

CAL formalization of delegation certificate:

- Certificate: K_I-$\langle \epsilon$/com : $K_{com} \rangle$
- CAL formalization: K_I **says** (K_{com} **speaksfor** ϵ/com)

Public Key Infrastructure (PKI)



PKI Excerpt

…
K_I-⟨ϵ/com : K_{com}⟩
K_I-⟨ϵ/edu : K_{edu}⟩
…

/

…
K_{edu}-⟨ϵ/edu/cu : K_{cu}⟩
K_{edu}-⟨ϵ/edu/mit : K_{mit}⟩
…

/edu

…
K_{cu}-⟨ϵ/edu/cu/cs : K_{cs}⟩
K_{cu}-⟨ϵ/edu/cu/ece : K_{ece}⟩
…

/edu/cu

…
K_{cs}-⟨ϵ/edu/cu/cs/fbs : K_{fbs}⟩
K_{cs}-⟨ϵ/edu/cu/cs/la : K_{la}⟩
…

/edu/cu/cs

CAL Model for PKI Excerpt

…
K_I-⟨ϵ/com : K_{com}⟩ ➡ K_I **says** (K_{com} **speaksfor** ϵ/com)
K_I-⟨ϵ/edu : K_{edu}⟩ ➡ K_I **says** (K_{edu} **speaksfor** ϵ/edu)
…

…
K_{edu}-⟨ϵ/edu/cu : K_{cu}⟩ ➡ K_{edu} **says** (K_{cu} **speaksfor** ϵ/edu/cu)
K_{edu}-⟨ϵ/edu/mit : K_{mit}⟩ ➡ K_{edu} **says** (K_{mit} **speaksfor** ϵ/edu/mit)
…

…
K_{cu}-⟨ϵ/edu/cu/cs : K_{cs}⟩ ➡ K_{cu} **says** (K_{cs} **speaksfor** ϵ/edu/cu/cs)
K_{cu}-⟨ϵ/edu/cu/ece : K_{ece}⟩ ➡ K_{cu} **says** (K_{ece} **speaksfor** ϵ/edu/cu/ece)
…

…
K_{cs}-⟨ϵ/edu/cu/cs/fbs : K_{fbs}⟩ ➡ K_{cs} **says** (K_{fbs} **speaksfor** ϵ/edu/cu/cs/fbs)
K_{cs}-⟨ϵ/edu/cu/cs/la : K_{la}⟩ ➡ K_{cs} **says** (K_{la} **speaksfor** ϵ/edu/cu/cs/la)
…

Sample Derivation

K_{fbs} **speaksfor** ϵ/edu/cu/cs/fbs

CAL Model for PKI Except

…
K_I-⟨ϵ/com : K_{com}⟩
K_I-⟨ϵ/edu : K_{edu}⟩ ➡ K_I **says** (K_{edu} **speaksfor** ϵ/edu)
…

…
K_{edu}-⟨ϵ/edu/cu : K_{cu}⟩ ➡ K_{edu} **says** (K_{cu} **speaksfor** ϵ/edu/cu)
K_{edu}-⟨ϵ/edu/mit : K_{mit}⟩
…

…
K_{cu}-⟨ϵ/edu/cu/cs : K_{cs}⟩ ➡ K_{cu} **says** (K_{cs} **speaksfor** ϵ/edu/cu/cs)
K_{cu}-⟨ϵ/edu/cu/ece : K_{ece}⟩
…

…
K_{cs}-⟨ϵ/edu/cu/cs/fbs : K_{fbs}⟩ ➡ K_{cs} **says** (K_{fbs} **speaksfor** ϵ/edu/cu/cs/fbs)
K_{cs}-⟨ϵ/edu/cu/ece/la : K_{la}⟩
…

Sample Derivation (1)

K_{fbs} **speaksfor** ϵ/edu/cu/cs/fbs

Sample Derivation (2)

K_{cs} **says** K_{fbs} **speaksfor** ϵ/edu/cu/cs/fbs

K_{CS} **speaksfor** ϵ/edu/cu/cs

ϵ/edu/cu/cs **says** K_{fbs} **speaksfor** ϵ/edu/cu/cs/fbs

ϵ/edu/cu/cs **speaksfor** ϵ/edu/cu/cs/fbs

ϵ/edu/cu/cs/fbs **says** K_{fbs} **speaksfor** ϵ/edu/cu/cs/fbs

K_{fbs} **speaksfor** ϵ/edu/cu/cs/fbs

Sample Derivation (3)

K_{CS} **speaksfor** ϵ/edu/cu/cs

K_{cs} **says** K_{fbs} **speaksfor** ϵ/edu/cu/cs/fbs

~~K_{CS} **speaksfor** ϵ/edu/cu/cs~~

ϵ/edu/cu/cs **says** K_{fbs} **speaksfor** ϵ/edu/cu/cs/fbs

ϵ/edu/cu/cs **speaksfor** ϵ/edu/cu/cs/fbs

ϵ/edu/cu/cs/fbs **says** K_{fbs} **speaksfor** ϵ/edu/cu/cs/fbs

K_{fbs} **speaksfor** ϵ/edu/cu/cs/fbs

Sample Derivation (4)

K_{cu} **says** K_{cs} **speaksfor** ϵ/edu/cu/cs

K_{cu} **speaksfor** ϵ/edu/cu

ϵ/edu/cu **says** K_{cs} **speaksfor** ϵ/edu/cu/cs

ϵ/edu/cu **speaksfor** ϵ/edu/cu/cs

ϵ/edu/cu/cs **says** K_{cs} **speaksfor** ϵ/edu/cu/cs

K_{CS} **speaksfor** ϵ/edu/cu/cs

K_{cs} **says** K_{fbs} **speaksfor** ϵ/edu/cu/cs/fbs

~~K_{CS} **speaksfor** ϵ/edu/cu/cs~~

ϵ/edu/cu/cs **says** K_{fbs} **speaksfor** ϵ/edu/cu/cs/fbs

ϵ/edu/cu/cs **speaksfor** ϵ/edu/cu/cs/fbs

ϵ/edu/cu/cs/fbs **says** K_{fbs} **speaksfor** ϵ/edu/cu/cs/fbs

K_{fbs} **speaksfor** ϵ/edu/cu/cs/fbs

Sample Derivation (5)

K_I **speaksfor** ϵ …

K_{cu} **says** K_{cs} **speaksfor** ϵ/edu/cu/cs

~~K_{cu} **speaksfor** ϵ/edu/cu~~

ϵ/edu/cu **says** K_{cs} **speaksfor** ϵ/edu/cu/cs

ϵ/edu/cu **speaksfor** ϵ/edu/cu/cs

ϵ/edu/cu/cs **says** K_{cs} **speaksfor** ϵ/edu/cu/cs

K_{CS} **speaksfor** ϵ/edu/cu/cs

K_{cs} **says** K_{fbs} **speaksfor** ϵ/edu/cu/cs/fbs

~~K_{CS} **speaksfor** ϵ/edu/cu/cs~~

ϵ/edu/cu/cs **says** K_{fbs} **speaksfor** ϵ/edu/cu/cs/fbs

ϵ/edu/cu/cs **speaksfor** ϵ/edu/cu/cs/fbs

ϵ/edu/cu/cs/fbs **says** K_{fbs} **speaksfor** ϵ/edu/cu/cs/fbs

K_{fbs} **speaksfor** ϵ/edu/cu/cs/fbs