# *Variations in Access Control Logic* Review

## Based on Martín Abadi's article

Luiz Cláudio F. Fernandez

lcfernandez@cos.ufrj.br

Programa de Engenharia de Sistemas e Computação - Inteligência Artificial
COPPE/UFRJ

Tópicos Especiais em Inteligência Artificial II 2015.2
Oct. 29, 2015

# Outline

# Introduction

- Investigate/design space of access control logics:
  - Formal consequences;
  - Security interpretations.
- Possible axioms for the commom operator `says`;
- Modal logic and programming-language theory ($\lambda$-calculus);
- Security:
  - Delegation of authority;
  - Principle of Least Privilege.
- Identifying logics that are sufficiently strong.

# Introduction

- Reduce access control to few central concepts and rules;
- The development/use of general logics is a ongoing effort;
- The logics all start from propositional logic with $\mathtt{says}$;
- They all allow the definition of a "speaks for" relation:

  $A$ speaks for $B$ if, for every $X$, if $A$ $\mathtt{says}$ $X$ then $B$ $\mathtt{says}$ $X$
- In a formula $A$ $\mathtt{says}$ $s$:
  - $A$ represents a principal;
  - $s$ represents a statement.

# Axioms

- Basic axioms of standard modal logic:
  - `says` is closed under consequence;
  - necessitation rule.
- Hand-off;
- Authority-shortcut;
- Unit;
- Bind;
- Escalation;
- Control-monotonicity.

# Results

- In classical logics:

$$\begin{tikzcd} \text{Unit} \arrow[d, Rightarrow] \\ \text{Escalation} \arrow[d, Leftrightarrow] \\ \text{Bind} \end{tikzcd}$$

- In intuitionistic logics:

$$\begin{tikzcd} \text{CDD} \arrow[d, Rightarrow] \arrow[dr, Rightarrow] & \text{Escalation} \arrow[d, Rightarrow] \\ \text{Unit} & \text{Bind} \end{tikzcd}$$

# Results

- (General) hand-off $\equiv$ Bind;
- Unit $\Rightarrow$ Authority-shortcut
  - Is equivalent if there is a truth-telling principal.
- Escalation $\Rightarrow$ Control-monotonicity
  - Control-monotonicity *and* C4 $\Rightarrow$ Escalation

# Formulas

$$s ::= \texttt{true} \mid (s \vee s) \mid (s \wedge s) \mid (s \rightarrow s) \mid A \texttt{ says } s \mid X \mid \forall X.s$$

where $A \in \mathcal{P}$ (principals), and $X$ ranges over a set of variables.

We write:

- $\texttt{false}$ for $\forall X.X$;
- $s_1 \equiv s_2$ for $(s_1 \rightarrow s_2) \wedge (s_2 \rightarrow s_1)$;
- $A \Rightarrow B$ for $\forall X.(A \texttt{ says } X \rightarrow B \texttt{ says } X)$ ["$A$ speaks for $B$"];
- $A \texttt{ controls } s$ for $(A \texttt{ says } s) \rightarrow s$.

# Basic Axioms and Rules

- Second-order, intuitionistic, multi-modal version of K:
  - Second-order propositional intuitionistic logic;
  - Closure under consequence axiom:

$$\forall X, Y.((A \text{ says } (X \to Y)) \to (A \text{ says } X) \to (A \text{ says } Y))$$

  - Necessitation rule: $$\frac{s}{A \text{ says } s}$$
- Classical variants:

$$[\textit{Excluded-middle}]\ \forall X.(X \vee (X \to \texttt{false}))$$

# CDD

- Adequate as a logic for access control;
- Is related to lax logic and the computational $\lambda$-calculus;
- In our context, CDD amounts to adopting:

$$[\mathit{Unit}]\ \forall X.(X \rightarrow A \texttt{ says } X)$$
$$[\mathit{Bind}]\ \forall X, Y((X \rightarrow A \texttt{ says } Y) \rightarrow (A \texttt{ says } X) \rightarrow (A \texttt{ says } Y))$$

# C4 in CDD

$$[C4]\ \forall X.(A \text{ says } A \text{ says } X \rightarrow A \text{ says } X)$$

- We can replace Bind with the simpler C4 when we have Unit:

**Proposition 1**

Starting from the basic logic (without Excluded-middle), we have:

1. *Bind implies C4;*
2. *Unit and C4 (together) imply Bind;*
3. *C4 does not imply Bind;*
4. *Unit does not imply C4 (and a fortiori not Bind).*

# C4 in CDD

**Proposition 2**

Starting from the basis logic plus Excluded-middle, we have:

1. *C4 implies neither Bind nor Unit;*
2. *Unit implies C4 (and therefore Bind);*
3. *Bind does not imply Unit.*

# Hand-off in CDD

- We obtain the hand-off axiom and a slight generalization as a theorem:

[*Hand-off*] $A$ `controls` $(B \Rightarrow A)$
[*Generalized-hand-off*] $\forall X, Y.A$ `controls` $(X \rightarrow A$ `says` $Y)$

**Theorem 1**

Starting from the basic logic:

*Bind is equivalent to Generalized-hand-off.*

# The Limits of Hand-off in CDD

- We define *Authority-shortcut*:

$$(\forall X.A \texttt{ controls } (A \texttt{ says } X \to B \texttt{ says } X)) \to (A \Rightarrow B)$$

**Theorem 2**

*Unit implies Authority-shortcut.*

# Escalation

$$[\mathit{Escalation}]\ \forall X, Y.((A \texttt{ says } X) \rightarrow (X \vee (A \texttt{ says } Y)))$$

$$|||$$

$$\forall X, Y.((A \texttt{ says } X) \rightarrow (X \vee (A \texttt{ says } \texttt{false})))$$

- Formally, we can derive:

$$(A \texttt{ controls } s) \wedge (B \texttt{ controls } s) \rightarrow ((A \texttt{ says } B \texttt{ says } s) \rightarrow s)$$

**Theorem 3**

Starting from the basic logic:

1. *Unit and Bind (together) do not imply Escalation;*
2. *Escalation implies Bind (and therefore C4).*

# Escalation

## Theorem 4

Starting from the basic logic plus Excluded-middle, we have:

1. *Unit implies Escalation (and therefore Bind);*
2. *Escalation (and a fortiori Bind) does not imply Unit;*
3. *Bind implies Escalation;*
4. *C4 does not imply Escalation.*

# On the Monotonicity of Controls

- If a pricipal controls a formula $X$, then it controls every weaker formula $Y$;
- Formally, we write *Control-monotonicity*:

$$\forall X, Y.((X \to Y) \to ((A \texttt{ controls } X) \to (A \texttt{ controls } Y)))$$

- Principle of Least Privilege:

*Every program and every user of the system should operate using the least set of privileges necessary to complete the job.*

# On the Monotonicity of Controls

## Proposition 3

Starting from the basic logic, Control-monotonicity implies:

$$A \texttt{ controls } s_1 \to A \texttt{ says } s_2 \to (s_1 \vee s_2)$$

## Theorem 5

Starting from the basic logic, the following are equivalent:

- *Escalation;*
- *C4 and Control-monotonicity.*

However, neither Control-monotonicity nor C4 implies the other, not even in combination with Unit.

# On the Monotonicity of Controls

**Theorem 6**

Starting from the basic logic plus Excluded-middle, the following are equivalent:

- *Escalation;*
- *Control-monotonicity.*

# Discussion

- In a intuitionistic setting we may adopt CDD (hand-off);
- Great deal of caution should be applied in selecting axioms;
- The literature contains models for some of these axioms;
- Semantics can be helpful in providing a different perspective;
- More extensive uses of semantics remain attractive.