# Opacity Control

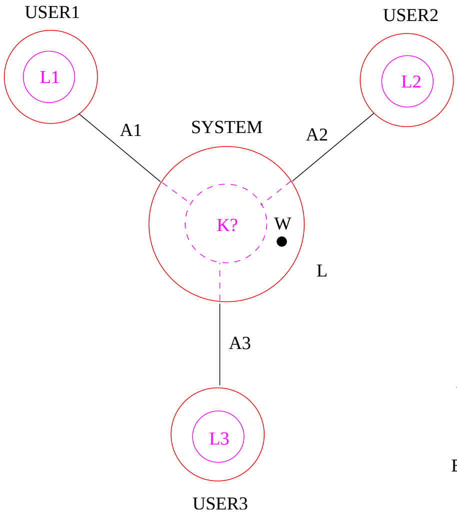
joint work with

E. Badouel     M. Bednarczyk
A. Borzyszkowski     B. Caillaud
*JDEDS 2007*

J. Dubreil     H. Marchand
*Wodes 2008 + new paper*

January 2009

# A Confidentiality Problem




Li IN Ai *

UNCONTROLLED BEHAVIOUR

L INCLUDED IN (A1+A2+A3) *

W IN L (RUN OF THE SYSTEM)

FIND MAXIMAL PERMISSIVE CONTROL

K INCLUDED IN L SUCH THAT

USERS i +1 AND i + 2 MAY NEVER KNOW

THAT THE Ai PROJECTION OF W IS IN Li

EVEN THOUGH THEY TALK TO EACH OTHER

# Formalization

SECRET SET

$$S_1 = (L_1 \parallel (A_2 + A_3)^*) \cap L$$
$$S_2 = (L_2 \parallel (A_1 + A_3)^*) \cap L$$
$$S_3 = (L_3 \parallel (A_1 + A_2)^*) \cap L$$

ADVERSARY'S ALPHABET

$$\Sigma_1 = A_2 \cup A_3$$
$$\Sigma_2 = A_1 \cup A_3$$
$$\Sigma_3 = A_1 \cup A_2$$

$\mathcal{S} = \{(S_1, \Sigma_1), (S_2, \Sigma_2), (S_3, \Sigma_3)\}$ is a CONCURRENT SECRET

**Definition**

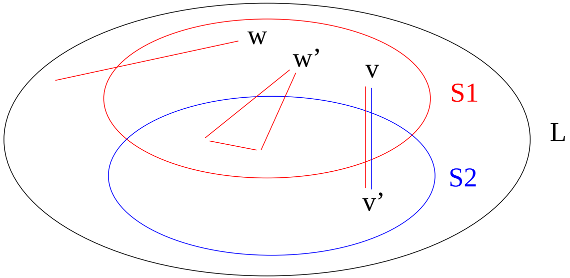
$\mathcal{S}$ is opaque if $\forall w \in L \;\; \forall i$
$w \in S_i \;\Rightarrow\; \Pi_{\Sigma_i}(w) = \Pi_{\Sigma_i}(w')$ for some $w' \in L \setminus S_i$

introduced by Laurent Mazare (with a single secret)

# Safe Kernels

**Definition**

The *safe kernel* $K(L, \mathcal{S})$ of $L$ is the subset of all words $w \in L$ such that for every prefix $u$ of $w$ and for every $i$
$\Pi_{\Sigma_i}(u) = \Pi_{\Sigma_i}(u')$ for some $u' \in L \setminus S_i$

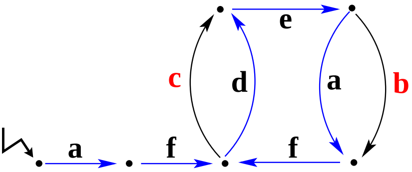



w in K(L,S)

w' not in K(L,S)

v,v' in K(L,S)

But using $K(L, \mathcal{S})$ as a controller does not solve our problem ...
because users know the system and the controller!




$S_1 = \Sigma^* afc(\Sigma \setminus \{c\})^*$ (last $c$ follows $af$), $\Sigma_1 = \{c, f\}$,
$S_2 = \Sigma^* deb(\Sigma \setminus \{b\})^*$ (last $b$ follows $de$), $\Sigma_2 = \{b, e\}$

$K(L, \mathcal{S}) = L \setminus afc\Sigma^*$
$K(K(L, \mathcal{S}), \mathcal{S}) = K(L, \mathcal{S}) \setminus afdeb\Sigma^*$

What remains in the end is $(afde)^*$

# Supremal Safe Sublanguage

$K(\bullet, \mathcal{S})$ is monotone in first argument

**Definition**

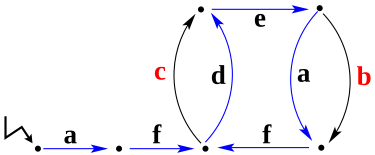
Let $SupK(L, \mathcal{S})$ be the greatest fixpoint of the operator $K(\bullet, \mathcal{S})$ included in $L$

**Theorem**

*$SupK(L, \mathcal{S})$ is the union of all controls enforcing the opacity of concurrent secret $\mathcal{S}$*

Sufficient conditions under which $SupK(L, \mathcal{S})$ is regular and computable ?

# $K(\bullet, \mathcal{S})$ may have a transfinite closure ordinal



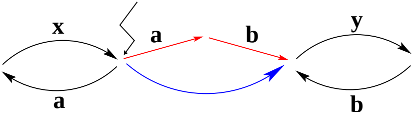

$S_1 = \Sigma^* afc(\Sigma \setminus \{c\})^*$ (last $c$ follows $af$), $\Sigma_1 = \{c, f\}$,
$S_2 = \Sigma^* deb(\Sigma \setminus \{b\})^*$ (last $b$ follows $de$), $\Sigma_2 = \{b, e\}$
$S_3 = L \setminus (\Sigma^* c \Sigma^*)$ (there is no $c$), $\Sigma_3 = \emptyset$
$S_3$ safe w.r.t. any $L' \subseteq L$ with at least one word with $c$

$$lim_{i \to \omega} K^i(L, \mathcal{S}) = Pref((afde)^\omega)$$

$$K^{\omega+1}(L, \mathcal{S}) = \emptyset$$

# $SupK(\bullet, \mathcal{S})$ may be not regular

$$\Sigma = \{a, b, x, y\} \quad L = Pref((ax)^*(\varepsilon + ab)(yb)^*)$$




$$\Sigma_1 = \{a, b\}, \quad \complement S_1 = \varepsilon + (ax)^* ab (yb)^* + \{a, x, y\}^*$$
$$\Sigma_2 = \{x, y\}, \quad \complement S_2 = (ax)^*(yb)^*$$
$$\Sigma_3 = \{a, b, x, y\}, \quad \complement S_3 = \varepsilon + a\Sigma^*$$

$S_1 = \color{blue}{\rightarrow}$ $\qquad$ $S_2 = \color{red}{\rightarrow\rightarrow}$

$S_2$ forces to start with $y$

$$SupK(L, \mathcal{S}) = Pref\left(\cup_{n \in \mathbb{N}} (ax)^n (\varepsilon + ab) (yb)^n\right)$$

# Some sufficient conditions

**language theoretic conditions (i) and (ii)**

i) system language L closed under prefix

ii) secrets closed under suffix ($S_i\Sigma^* \subseteq S_i$)

**structural conditions (iii) or (iv) or (v)**

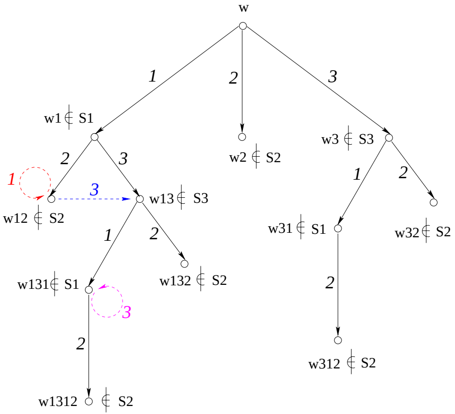
iii) $\Sigma_1 \subseteq \Sigma_2 \ldots \subseteq \Sigma_n$ — chain of alphabets

iv) $S_1 \subseteq S_2 \ldots \subseteq S_n$ — chain of secrets

v) $(\forall i \neq j)\ (\forall w, w' \in L)$ — observers $\perp$ secrets

$\Pi_{\Sigma_j}(w) = \Pi_{\Sigma_j}(w') \Rightarrow w \in S_i$ iff $w' \in S_i$ — true in first Example

$S_1 \subseteq S_2 \quad \Sigma_3 \subseteq \Sigma_2 \quad Obs_1 \perp S_3$ (mixed case)




Finite pattern of proofs for $w \in SupK(L, \mathcal{S})$

$w, w_i, w_{ij}, w_{ijk}, w_ijkl \in L$

**Theorem**

*It is decidable whether there exists a finite uniform pattern of proofs for all $w \in SupK(L, \mathcal{S})$*

Under this condition, one can construct a finite automaton accepting $SupK(L, \mathcal{S})$

Moreover $SupK(L, \mathcal{S})$ is totally determined by its projections on the $\Sigma_i$, hence we obtain

Decentralized Control

# Ramadge and Wonham supervisory control

Partial Observation: $\Sigma = \Sigma_o \cup \Sigma_{uo}$
Partial Controllability: $\Sigma = \Sigma_c \cup \Sigma_{uc}$
Special Case: $\Sigma_c \subseteq \Sigma_o$

$K \subseteq L$ is an admissible controller if
$K$ is prefix-closed
$K$ is controllable w.r.t. $L$: $K\Sigma_{uc} \cap L \subseteq K$
$K$ is normal w.r.t. $L$: $K = \pi_o^{-1} \circ \pi_o(K) \cap L$

if $L' \subseteq L$ are regular, the most permissive controller
$K = \mathit{SupCN}(L', L)$ such that $L \cap K \subseteq L'$ is regular

# Supervisory control for simple opacity

$S \subseteq L \subseteq \Sigma^*$ SECRET
$\Sigma_a \subseteq \Sigma$ ADVERSARY'S ALPHABET
$\Sigma_c \subseteq \Sigma_o \subseteq \Sigma$ CONTROLLER'S ALPHABETS

The family of prefix-closed Controllable and Normal sublanguages $K$ of $L$ such that $S$ is Opaque w.r.t. $K$ has a Supremum $SupCNO(L, S)$

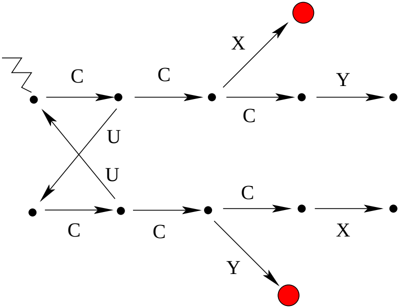
How computing $SupCNO(L, S)$?

Alternated greatest fixpoint iterations
$\ldots SupCN \circ SupO \circ SupCN \circ SupO \ldots$

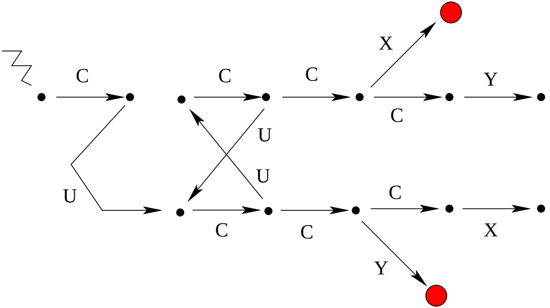
# An Example

$$\Sigma_a = \{C, X, Y\}$$
$$\Sigma_o = \{C, X, Y, U\}$$
$$\Sigma_c = \{C\}$$

SECRET disclosed by CCX but not by CUCCY

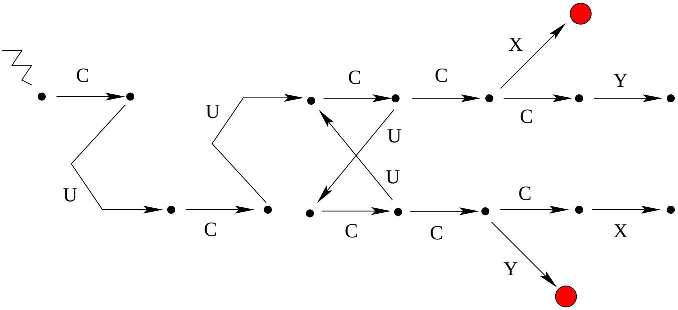


# First Iteration




SECRET disclosed by CUCCY but not by CUCUCCX

# Second Iteration




SECRET disclosed by CUCUCCX but not by CUCUCUCCY

# Wodes 2008

The alternated iteration terminates if
$\Sigma_c \subseteq \Sigma_o \subseteq \Sigma_a$ or $\Sigma_a \subseteq \Sigma_c \subseteq \Sigma_o$

Different method proposed for the case $\Sigma_c \subseteq \Sigma_a \subseteq \Sigma_o$

Given an automaton $G$ on $\Sigma$ generating $L$ and recognizing $S$,
replace $G$ with $G \times Det_{\Sigma_a}(G)$
and apply Ramadge and Wonham methods

States of the controller are pairs $(q, E)$
$q \in Q$ state of $G$
$E \subseteq Q$ adversary's estimate of the state of $G$.

# Further results

Does not work when $\Sigma_c$ not included in $\Sigma_a$

the estimate of the state of $G$ reached after $w$
depends on the controller $K$
and not only on $G$ and the $\Sigma_a$ projection of $w$

Consider all pairs $(q, E)$ even though
not accessible in $G \times Det_{\Sigma_a}(G)$

Revise the estimation $E$ of $q$ after $w$ for all $w$
at each step in the computation of $K^\dagger$

Yields a finite controller as desired

# PERSPECTIVES

Deal with simple opacity in the case where $\Sigma_a$ and $\Sigma_o$ do not compare

Deal with concurrent secrets $\mathcal{S} = \{(S_1, \Sigma_1), \dots, (S_i, \Sigma_i)\}$ where user $i$ observes $\Sigma_i \subseteq \Sigma$ and controls $\Sigma_{c,i} \subseteq \Sigma_i$

Strategies for disclosing the secrets of the others while keeping one's secret safe?

Opacity not expressible in MSO (Alur)!