Verification of Information Flow Properties under Rational Observation

Béatrice Bérard[1] John Mullins[2]

[1]Université Pierre & Marie Curie, LIP6/MoVe, CNRS UMR 7606
[2]École Polytechnique de Montral

Work partially supported by Coopération France-Québec - 2012/26/SCAC and

AVOCS
September 24th, 2014

Context: Verification of Security Properties

Information flow:

Transmission of information from a high level user to a low level user,
in a possibly illegal and/or indirect way.

A class of Security Properties:

Avoid information flow to preserve secret data during communications.
[Mantel 2000, Focardi, Gorrieri 2001, Bryans, Koutny, Mazaré, Ryan 2008].

Goal:

Check whether a system satisfies such properties.
[BKMR 2008, D'Souza, Holla, Raghavendra, Sprick 2011, Best, Darondeau, Gorrieri 2011, Best, Darondeau 2012, Cassez, Dubreil, Marchand 2012, Dimitrova, Finkbeiner, Kovács, Rabe, Seidl 2012, Clarkson, Finkbeiner, Koleini, Micinski, Rabe, Sanchez 2014]

Our setting:

System behaviour described by a language = set of traces

Examples

Given an alphabet A and a language $L \subseteq A^*$

- $A = V \uplus C \uplus N$ a partition into visible, confidential and neutral actions.

Removal of confidential actions:

An observer cannot see if the confidential actions are erased: for any $w \in L$, erasing all confidential actions in w results in a behaviour still in L.

Examples

Given an alphabet A and a language $L \subseteq A^*$

- $A = V \uplus C \uplus N$ a partition into visible, confidential and neutral actions.

Removal of confidential actions:

An observer cannot see if the confidential actions are erased: for any $w \in L$, erasing all confidential actions in w results in a behaviour still in L.

Insertion of X-admissible confidential actions, with $X \subseteq A$:

for any $w = w_1 w_2 \in L$ such that w_2 contains no confidential event and there exists $w_3 \in A^*$ and $c \in C$ with $w_3 c \in L$ and the X-letters in w_1 and w_3 are the same, then $w_1 c w_2$ also belongs to L.

Examples

Given an alphabet A and a language $L \subseteq A^*$

- $A = V \uplus C \uplus N$ a partition into visible, confidential and neutral actions.

Removal of confidential actions:

An observer cannot see if the confidential actions are erased: for any $w \in L$, erasing all confidential actions in w results in a behaviour still in L.

Insertion of X-admissible confidential actions, with $X \subseteq A$:

for any $w = w_1 w_2 \in L$ such that w_2 contains no confidential event and there exists $w_3 \in A^*$ and $c \in C$ with $w_3 c \in L$ and the X-letters in w_1 and w_3 are the same, then $w_1 c w_2$ also belongs to L.

- $A = V \uplus P$ a partition into visible actions and participant actions.

Strong anonymity of participants:

for any $w \in L$, replacing in w an action $a \in P$ by any other action in P produces a behaviour still in L.

Examples

Given an alphabet A and a language $L \subseteq A^*$

- $A = V \uplus C \uplus N$ a partition into visible, confidential and neutral actions.

Removal of confidential actions:

An observer cannot see if the confidential actions are erased: for any $w \in L$, erasing all confidential actions in w results in a behaviour still in L.

Insertion of X-admissible confidential actions, with $X \subseteq A$:

for any $w = w_1 w_2 \in L$ such that w_2 contains no confidential event and there exists $w_3 \in A^*$ and $c \in C$ with $w_3 c \in L$ and the X-letters in w_1 and w_3 are the same, then $w_1 c w_2$ also belongs to L.

- $A = V \uplus P$ a partition into visible actions and participant actions.

Strong anonymity of participants:

for any $w \in L$, replacing in w an action $a \in P$ by any other action in P produces a behaviour still in L.

- $\varphi \subseteq L$ a subset of secret behaviours.

Opacity of φ in L:

any behaviour in φ is observed identically to another behaviour not in φ.

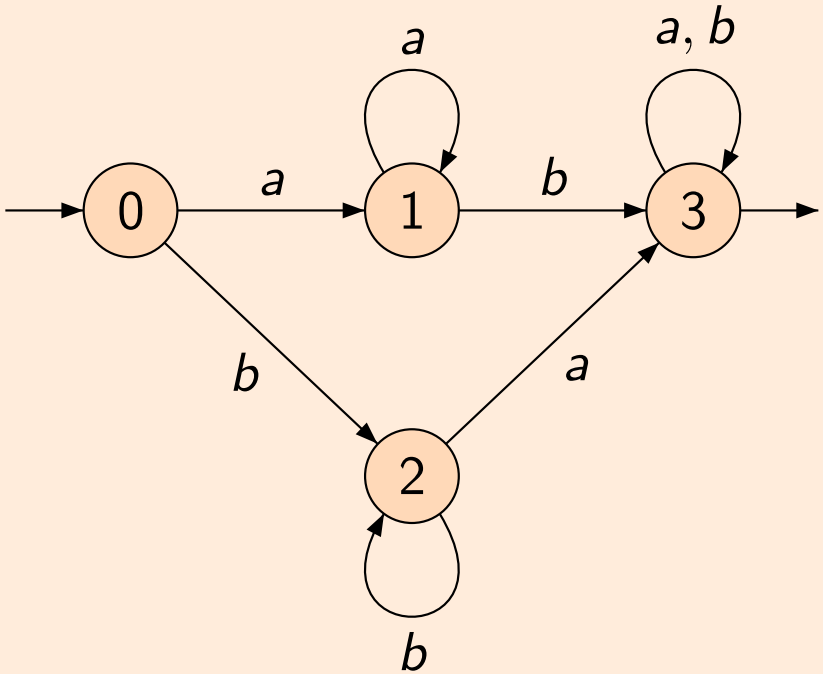
Outline

Rational Information Flow Properties

General results

Finite automata and finite transducers

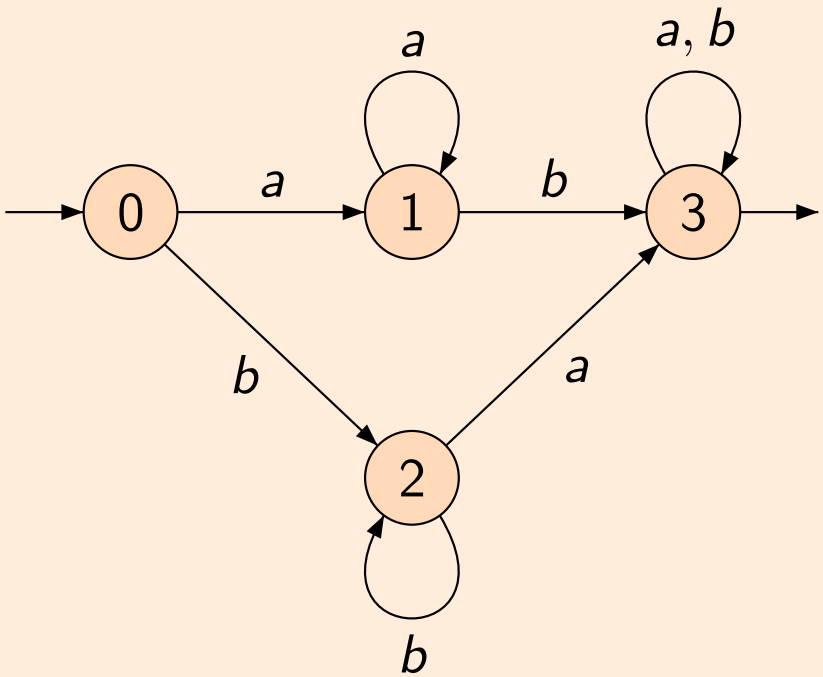
- An automaton is a finite Labelled Transition System over a set of labels Lab. With final states and Lab is alphabet A, it accepts a regular language in A^*.

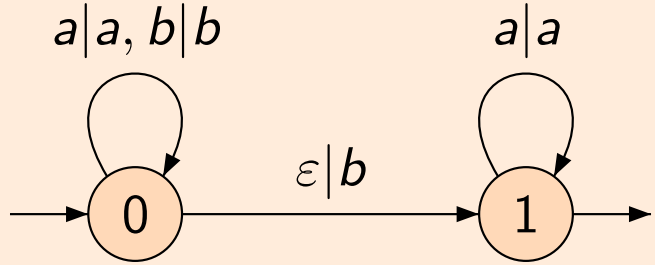


$L = a^+ b\{a, b\}^* \cup b^+ a\{a, b\}^*$

Finite automata and finite transducers

- An automaton is a finite Labelled Transition System over a set of labels Lab. With final states and Lab is alphabet A, it accepts a regular language in A^*.
- A transducer is an automaton with set of labels $Lab \subseteq A^* \times B^*$. With final states, it accepts a rational relation in $A^* \times B^*$.



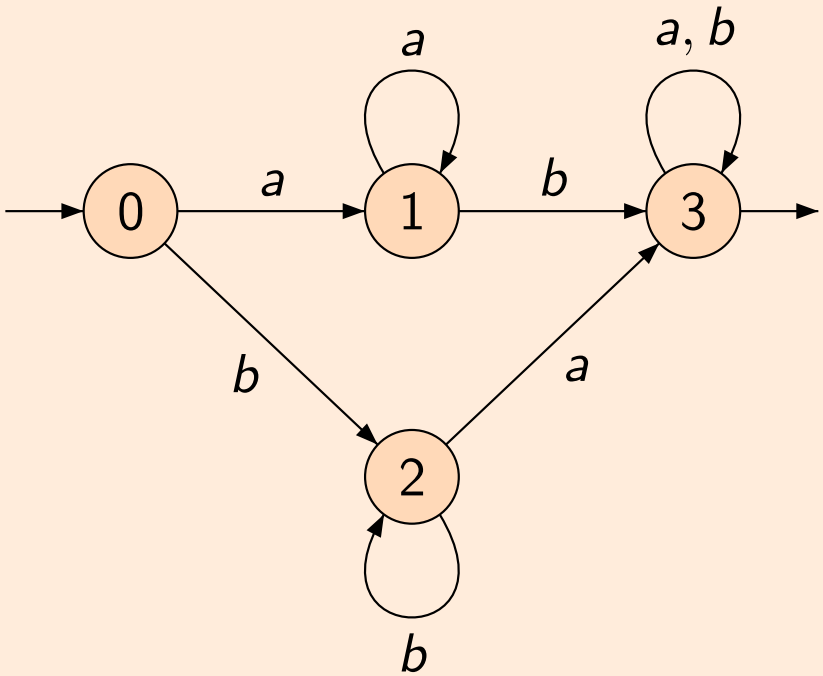


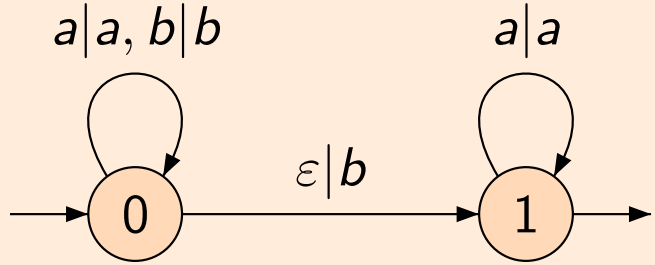
$L = a^+ b\{a, b\}^* \cup b^+ a\{a, b\}^*$

$R = \{(a, a), (b, b)\}^*(\varepsilon, b)(a, a)^*$

Finite automata and finite transducers

- An automaton is a finite Labelled Transition System over a set of labels Lab. With final states and Lab is alphabet A, it accepts a regular language in A^*.
- A transducer is an automaton with set of labels $Lab \subseteq A^* \times B^*$. With final states, it accepts a rational relation in $A^* \times B^*$.





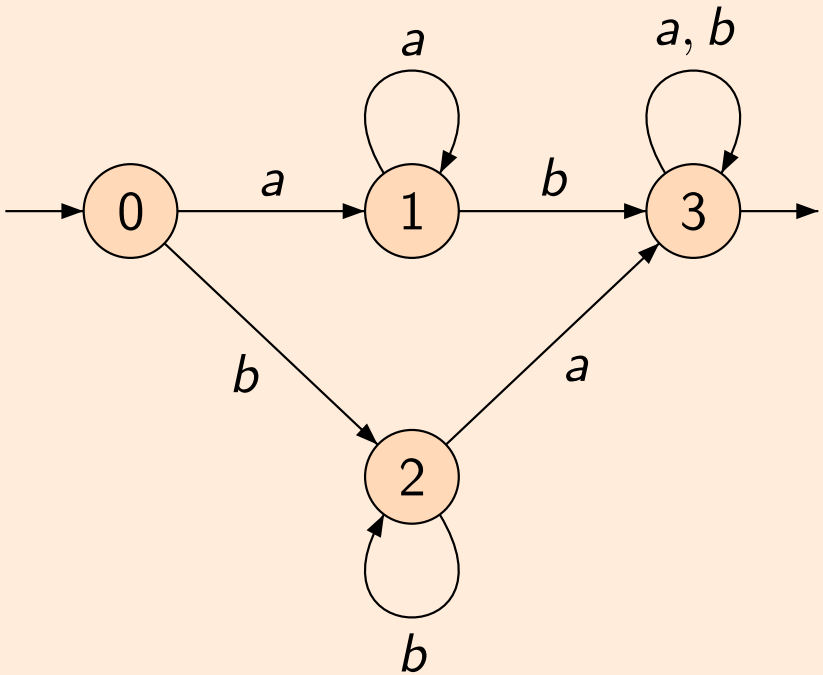
$abaaa \rightarrow abbaaa$

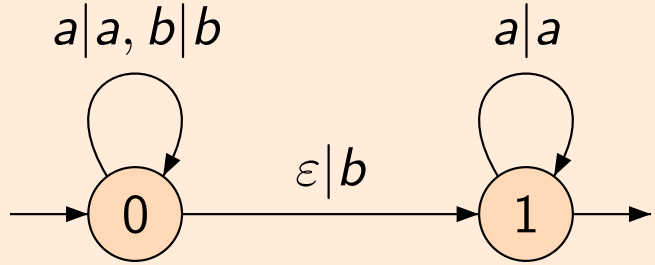
$L = a^+b\{a,b\}^* \cup b^+a\{a,b\}^*$

$R = \{(a,a),(b,b)\}^*(\varepsilon,b)(a,a)^*$

Finite automata and finite transducers

- An automaton is a finite Labelled Transition System over a set of labels Lab. With final states and Lab is alphabet A, it accepts a regular language in A^*.
- A transducer is an automaton with set of labels $Lab \subseteq A^* \times B^*$. With final states, it accepts a rational relation in $A^* \times B^*$.





$abaaa \rightarrow abbaaa$
$ababaa$
$abaaba$
$abaaab$

$L = a^+b\{a,b\}^* \cup b^+a\{a,b\}^*$

$R = \{(a,a),(b,b)\}^*(\varepsilon,b)(a,a)^*$

Rational observers and RIFPs

A rational observer

is a rational relation $\mathcal{O} \subseteq A^* \times B^*$.
Observation of $w \in A^*$: $\mathcal{O}(w) = \{w' \in B^* \mid (w, w') \in \mathcal{O}\}$.
Observation of $L \subseteq A^*$: $\mathcal{O}(L) = \cup_{w \in L} \mathcal{O}(w)$

A rational information flow property (RIFP) for language L

is any relation $L_1 \subseteq L_2$, where L_1 and L_2 are given by:

$$L_1, L_2 ::= \; L \mid \mathcal{O}(L_1) \mid L_1 \cup L_2 \mid L_1 \cap L_2$$

where $\mathcal{O}$ is a rational observer.

$RIF(\mathcal{L})$ for a class of languages $\mathcal{L}$

is the set of rational information flow properties for languages $L \in \mathcal{L}$.

Example 1: Removal of confidential actions

$A = V \uplus C \uplus N$ a partition into visible, confidential and neutral actions.

An observer cannot see if the confidential actions are erased: for any behaviour $w \in L$, erasing all confidential actions in w results in a behaviour still in L.

Translates as

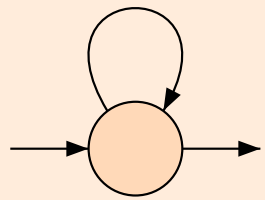
$$\pi_{\overline{C}}(L) \subseteq L$$

where $\pi_{\overline{C}}$ is the projection from A^* onto $(A \setminus C)^*$:

A morphism such that

$$\pi_{\overline{C}}(a) = \begin{cases} \varepsilon \text{ if } a \in C \\ a \text{ otherwise} \end{cases}$$

$c|\varepsilon, c \in C$
$a|a, a \in V \uplus N$



Example 1: Removal of confidential actions

$A = V \uplus C \uplus N$ a partition into visible, confidential and neutral actions.

An observer cannot see if the confidential actions are erased: for any behaviour $w \in L$, erasing all confidential actions in w results in a behaviour still in L.

Translates as

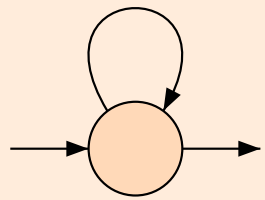
$$\pi_{\overline{C}}(L) \subseteq L$$

where $\pi_{\overline{C}}$ is the projection from A^* onto $(A \setminus C)^*$:

A morphism such that

$$\pi_{\overline{C}}(a) = \begin{cases} \varepsilon \text{ if } a \in C \\ a \text{ otherwise} \end{cases}$$

$c|\varepsilon, c \in C$
$a|a, a \in V \uplus N$



Proposition

Since $\pi_{\overline{C}}$ is a rational observer, removal of confidential actions is an RIFP.

Example 2: Insertion of confidential actions

$A = V \uplus C \uplus N$ and $X \subseteq A$.

For any $w = w_1 w_2 \in L$ such that w_2 contains no confidential event and there exists $w_3 \in A^*$ and $c \in C$ with $w_3 c \in L$ and the X-letters in w_1 and w_3 are the same, then $w_1 c w_2$ also belongs to L.

Translates as

$$\bigcup_{c \in C} (l\text{-}ins_c(L) \cap \mathcal{O}_c^X(L)) \subseteq L$$

where for each $c \in C$,

- $l\text{-}ins_c$ is the rational relation inserting c after the last confidential action,
- $\mathcal{O}_c^X$ is defined by $\mathcal{O}_c^X(u) = \pi_X^{-1}(\pi_X(c^{-1}u)).c.(V \uplus N)^*$ for $u \in A^*$.

Example 2: Insertion of confidential actions

$A = V \uplus C \uplus N$ and $X \subseteq A$.

For any $w = w_1 w_2 \in L$ such that w_2 contains no confidential event and there exists $w_3 \in A^*$ and $c \in C$ with $w_3 c \in L$ and the X-letters in w_1 and w_3 are the same, then $w_1 c w_2$ also belongs to L.

Translates as

$$\bigcup_{c \in C} (l\text{-}ins_c(L) \cap \mathcal{O}_c^X(L)) \subseteq L$$

where for each $c \in C$,

- $l\text{-}ins_c$ is the rational relation inserting c after the last confidential action,
- $\mathcal{O}_c^X$ is defined by $\mathcal{O}_c^X(u) = \pi_X^{-1}(\pi_X(c^{-1}u)).c.(V \uplus N)^*$ for $u \in A^*$.

Proposition

All operations are rational observers, hence insertion of X-admissible confidential actions is an RIFP.

Example 3: Strong anonymity

$A = V \uplus P$.

For any $w \in L$, replacing in w an action in P by another produces a behaviour in L.

Translates as

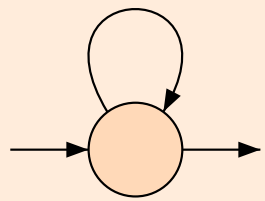
$$\mathcal{O}^P_{SA}(L) \subseteq L$$

where $\mathcal{O}^P_{SA}$ is a substitution:

A morphism such that

$$\mathcal{O}^P_{SA}(a) = \begin{cases} P \text{ if } a \in P \\ \{a\} \text{ otherwise} \end{cases}$$

$v|v, v \in V$
$a|a', \ (a, a') \in P \times P$



Example 3: Strong anonymity

$A = V \uplus P$.

For any $w \in L$, replacing in w an action in P by another produces a behaviour in L.

Translates as

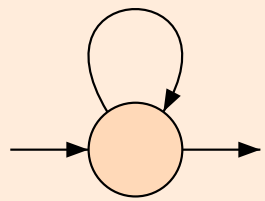
$$\mathcal{O}^P_{SA}(L) \subseteq L$$

where $\mathcal{O}^P_{SA}$ is a substitution:

A morphism such that

$$\mathcal{O}^P_{SA}(a) = \begin{cases} P \text{ if } a \in P \\ \{a\} \text{ otherwise} \end{cases}$$

$v|v, v \in V$
$a|a', \ (a, a') \in P \times P$



Proposition

A substitution is a rational observer, hence strong anonymity is an RIFP.

Verification of RIFPs

For a class of languages $\mathcal{L}$:

If $\mathcal{L}$ is closed under union, intersection, and rational transductions, and if the inclusion is decidable in $\mathcal{L}$, then any property in $RIF(\mathcal{L})$ is decidable.

Verification of RIFPs

For a class of languages $\mathcal{L}$:

If $\mathcal{L}$ is closed under union, intersection, and rational transductions, and if the inclusion is decidable in $\mathcal{L}$, then any property in $RIF(\mathcal{L})$ is decidable.

For the class $\mathcal{R}eg$ of regular languages:

The problem of deciding a property in $RIF(\mathcal{R}eg)$ is PSPACE-complete.

Because regular languages have all the required closure properties and inclusion is decidable in PSPACE in $\mathcal{R}eg$.
PSAPCE-hardness comes from the fact that $\mathcal{O}_K(w) = \{w\} \cap K$ is a rational relation if and only if K is a regular language.

Verification of RIFPs

For a class of languages $\mathcal{L}$:

If $\mathcal{L}$ is closed under union, intersection, and rational transductions, and if the inclusion is decidable in $\mathcal{L}$, then any property in $RIF(\mathcal{L})$ is decidable.

For the class $\mathcal{R}eg$ of regular languages:

The problem of deciding a property in $RIF(\mathcal{R}eg)$ is PSPACE-complete.

Because regular languages have all the required closure properties and inclusion is decidable in PSPACE in $\mathcal{R}eg$.
PSAPCE-hardness comes from the fact that $\mathcal{O}_K(w) = \{w\} \cap K$ is a rational relation if and only if K is a regular language.

Consequence:

Strong (and weak) anonymity [BKMR 2008], as well as all Basic Security Predicates [Mantel 2000], are decidable (in PSPACE) for regular languages. We retrieve results from [D'Souza et al., 2011].

Verification of Opacity

$\varphi \subseteq L$ a subset of secret behaviours

Any behaviour in φ is observed identically as another behaviour not in φ.

Restricted to rational observation functions:

Rational opacity

Given a rational function $\mathcal{O}$ as observer, the secret φ is rationally opaque in L for $\mathcal{O}$ if

$$\mathcal{O}(\varphi) \subseteq \mathcal{O}(L \setminus \varphi)$$

Verification of Opacity

$\varphi \subseteq L$ a subset of secret behaviours

Any behaviour in φ is observed identically as another behaviour not in φ.

Restricted to rational observation functions:

Rational opacity

Given a rational function $\mathcal{O}$ as observer, the secret φ is rationally opaque in L for $\mathcal{O}$ if

$$\mathcal{O}(\varphi) \subseteq \mathcal{O}(L \setminus \varphi)$$

For regular secrets:

Rational opacity for regular secrets is an RIFP.

Consequence:

We retrieve the decidability result (in PSPACE) for rational opacity with regular languages and regular secrets [Cassez et al., 2012].

Declassification and revocation

Selective declassification (SD)

$A = V \uplus C \uplus D$, where actions in D indicate declassification of confidential actions
Each $d \in D$ declassifies a subset $C(d)$ of C.

Selective revocation

$A = V \uplus P \uplus R$, where actions in R indicate revocation of anonymity for participant actions in P
The subsets $P(r)$, of actions subject to revocation by $r \in R$, form a partition of P.

Declassification and revocation

Selective declassification (SD)

$A = V \uplus C \uplus D$, where actions in D indicate declassification of confidential actions
Each $d \in D$ declassifies a subset $C(d)$ of C.

Selective revocation

$A = V \uplus P \uplus R$, where actions in R indicate revocation of anonymity for participant actions in P
The subsets $P(r)$, of actions subject to revocation by $r \in R$, form a partition of P.

Proposition

Both selective declassification and selective revocation are rational observers, hence all related properties are RIFPs.
This applies to Intransitive Non Interference for SD (INISD) [BD12] and conditional anonymity.

Selective declassification

Example: $D = \{d_1, d_2\}$

Consider the last occurrence of d_1, d_2 in words of L:

5 possible declassification patterns $\Sigma = \{\varepsilon, d_1, d_2, d_1 d_2, d_2 d_1\}$

- $\sigma = \varepsilon$: w contains no action in D, then all confidential actions are invisible

$$\mathcal{O}_{SD}(w) = \pi_{V \uplus D}(w)$$

- $\sigma = d_1$: w contains occurrences of d_1 but not of d_2.

$$w : \overbrace{\qquad}^{w_1} d_1 \overbrace{\qquad}^{w_2} \qquad \mathcal{O}_{SD}(w) = \pi_{V_1}(w_1) d_1 \pi_V(w_2)$$

$V_1 = V \cup \{d_1\} \cup C(d_1)$ $\qquad$ V

- $\sigma = d_1 d_2$: last occurrence of d_1 precedes last occurrence of d_2.

$$w : \overbrace{\qquad}^{w_1} d_1 \overbrace{\qquad}^{w_2} d_2 \overbrace{\qquad}^{w_3}$$

$V_1 = V \cup \{d_1, d_2\} \cup C(d_1) \cup C(d_2)$ $\quad$ $V_2 = V \cup \{d_2\} \cup C(d_2)$ $\quad$ V

$$\mathcal{O}_{SD}(w) = \pi_{V_1}(w_1) d_1 \pi_{V_2}(w_2) d_2 \pi_V(w_3)$$

An Orwellian observer for SD

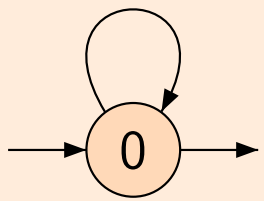
Example: $D = \{d_1, d_2\}$

$$\mathcal{O}_{SD} = \mathcal{O}_\varepsilon \uplus \mathcal{O}_{d_1} \uplus \mathcal{O}_{d_2} \uplus \mathcal{O}_{d_1 d_2} \uplus \mathcal{O}_{d_2 d_1}$$

A sum of 5 functions with disjoint supports, one for each declassification pattern.

$v|v, v \in V \cup D$
$c|\varepsilon, c \in C$

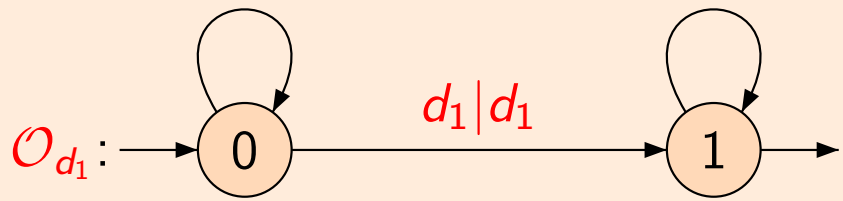
$\mathcal{O}_\varepsilon$:



$v|v, v \in V \cup \{d_1\} \cup C(d_1)$
$c|\varepsilon, c \in C \setminus C(d_1)$

$v|v, v \in V$
$c|\varepsilon, c \in C$

$\mathcal{O}_{d_1}$:



$v|v, v \in V \cup \{d_1, d_2\} \cup C(d_1) \cup C(d_2)$
$c|\varepsilon, c \in C \setminus (C(d_1) \cup C(d_2))$

$v|v, v \in V \cup \{d_2\} \cup C(d_2)$
$c|\varepsilon, c \in C \setminus C(d_2)$

$v|v, v \in V$
$c|\varepsilon, c \in C$

$\mathcal{O}_{d_1 d_2}$:

Conclusion

Contribution

- We introduce rational information flow properties, based on rational transducers for observations.
- We show that most properties defined up to now can be expressed as RIFPs.
- We give a generic result proving that RIFPs can be decided in PSPACE on regular languages.

Future work

- Identify other classes of languages $\mathcal{L}$ with similar properties.
- Link our verification results with those based on model checking extensions of LTL like SecLTL [DFKRS12] or even CTL* like HyperCTL* [CFKMRS14].

Thank you