

Interprétation logique de politiques de sécurité

Travail en cours ...

T. Bourdier^{1,2} H. Cirstea² M. Jaume³ H. Kirchner¹

¹ INRIA Grand Est & Sud-Ouest

² Nancy Université & LORIA,

³ SPI - LIP6 - Université Paris 6

27 Mai 2009

- **LTS** (*Labelled Transition System*) $(\mathcal{E}, \mathcal{E}_0, \mathcal{L}, \delta)$
 - ▶ \mathcal{E} : ensemble d'états
 - ▶ $\mathcal{E}_0 \subseteq \mathcal{E}$: ensemble d'états initiaux
 - ▶ \mathcal{L} : ensemble d'étiquettes
 - ▶ $\delta \subseteq \mathcal{E} \times \mathcal{L} \times \mathcal{E}$: relation de transition
- Appliquer une politique à un système : restreindre la relation de transition.
 - ▶ **Politique** : spécifiée par une relation $\mathcal{R} \subseteq \text{Pré} \times \mathcal{L} \times \text{Post}$
 - ★ $(P_1, \gamma, P_2) \in \mathcal{R}$: la transition d'étiquette γ est autorisée par la politique ssi elle est effectuée à partir d'un état vérifiant P_1 et conduit à un état vérifiant P_2
 - ▶ **Système restreint par une politique** : on conserve dans la relation de transition δ uniquement les éléments (e_1, γ, e_2) autorisés par la politique

Systemes et Politiques : Approche logique

- *Spécification de l'ensemble des états (i.e. des environnements)*
 - ▶ Les états sont décrits par une spécification (signature + théorie).
 - ▶ Un état est un modèle de la spécification.
- *Propriétés sur les états*
 - ▶ Les propriétés sur les états sont exprimées par un ensemble de formules sur la signature de la spécification.
 - ▶ Les états qui vérifient ces propriétés sont des modèles de cet ensemble de formules.

Signatures - Spécifications

- **Signature** : $\Sigma = (\mathcal{S}, \mathcal{F}, \mathcal{P})$
 - ▶ \mathcal{S} : ensemble de sortes
 - ▶ \mathcal{F} : ensemble de symboles de fonctions
 - ▶ \mathcal{P} : ensemble de symboles de prédicats
- **Spécification** : $\mathbb{SP} = (\Sigma, \mathbb{T})$
 - ▶ $\Sigma = (\mathcal{S}, \mathcal{F}, \mathcal{P})$: Signature
 - ▶ \mathbb{T} : Théorie (ensemble de Σ -formules)
- *Exemple.* $\Sigma_{BLP} = (\mathcal{S}_{BLP}, \mathcal{F}_{BLP}, \mathcal{P}_{BLP})$

$$\mathcal{S}_{BLP} = \{S, O, A, L\} \quad \mathcal{F}_{BLP} = \left\{ \begin{array}{l} read : \mapsto A \\ write : \mapsto A \\ f_s : S \mapsto L \\ f_o : O \mapsto L \end{array} \right\} \quad \mathcal{P}_{BLP} = \left\{ \begin{array}{l} inf : L, L \\ m : S, O, A \end{array} \right\}$$

$\mathbb{SP}_{BLP} = (\Sigma_{BLP}, \mathbb{T}_{BLP})$ où \mathbb{T}_{BLP} est une théorie exprimant que (L, inf) est un treillis.

Algèbres

- Σ -Algèbre \mathcal{A} :

- ▶ Pour chaque sorte $s \in \mathcal{S}$, A^s est le domaine d'interprétation de s
- ▶ Pour chaque symbole de fonction $f : s_1, \dots, s_n \mapsto s \in \mathcal{F}$, $f_{\mathcal{A}}$ est une fonction de $A^{s_1} \times \dots \times A^{s_n}$ dans A^s
- ▶ Pour chaque symbole de prédicat $p : s_1, \dots, s_n \in \mathcal{P}$,
 $p_{\mathcal{A}} \subseteq A^{s_1} \times \dots \times A^{s_n}$.

Alg_{Σ} : Σ -Algèbres

- Algèbres basées sur les constantes :

- ▶ les domaines d'interprétations correspondent aux constantes de la signature
- ▶ chaque constante est interprétée par elle-même

- Alg_{Σ_0} : Σ -Algèbres basées sur les constantes.

Etats

- Une Σ -algèbre \mathcal{A} est un modèle d'une spécification $\mathbb{SP} = (\Sigma, \mathbb{T})$ ssi \mathcal{A} est modèle de toutes les formules de \mathbb{T} .
- $\mathcal{Env}_{\mathbb{SP}}$: états décrits par une spécification $\mathbb{SP} = (\Sigma, \mathbb{T})$
 - ▶ Σ -algèbres basées sur les constantes qui sont modèles de \mathbb{SP}
- *Extension d'une spécification par un ensemble de constantes*
 - ▶ $\mathbb{SP}[\mathcal{C}] = (\Sigma[\mathcal{C}], \mathbb{T})$
 - ▶ $\Sigma[\mathcal{C}] = (\mathcal{S}, \mathcal{F} \cup \mathcal{C}, \mathcal{P})$

Permet de prendre en compte les constantes d'un domaine particulier dans le domaine d'interprétation (Alice, Bob, ...).

Requêtes, Décisions

- Une politique spécifie quelles décisions sont prises lorsque des requêtes sont soumises au système.
 - ▶ Les étiquettes du système sont des couples (requête,décision)
- Evènements
 - ▶ Signature : $\Sigma = (S, \mathcal{F}, \mathcal{P})$
 - ▶ $\Sigma_{EV} = (\{Query, Decision\} \cup S, \mathcal{F}_{EV} \cup \mathcal{F}, \emptyset)$
Le co-domaine des symboles de \mathcal{F}_{EV} est dans $\{Query, Decision\}$.
 - ▶ **Requêtes** : $\mathcal{Q}_{EV} = T_{\Sigma_{EV}}^{Query}$
 - ▶ **Décisions** : $\mathcal{D}_{EV} = T_{\Sigma_{EV}}^{Decision}$
 - ▶ **Evènements** : $\mathcal{L}_{EV} = \mathcal{Q}_{EV} \times \mathcal{D}_{EV}$
- Exemple. $\Sigma_{EV}^{BLP} = (\{Q, D\} \cup S_{BLP}, \mathcal{F}_{EV}^{BLP} \cup \mathcal{F}_{BLP}, \emptyset)$

$$\mathcal{F}_{EV}^{BLP} = \left\{ \begin{array}{ll} ask : S, O, A \mapsto Q, & permit : \mapsto D, \\ release : S, O, A \mapsto Q, & deny : \mapsto D \end{array} \right\}$$

Frames – Systèmes

- **Frame** : $\mathfrak{F} = (\mathbb{S}\mathbb{P}, \Sigma_{Ev})$
 - ▶ $\mathbb{S}\mathbb{P} = (\Sigma, \mathbb{T})$: spécification
 \rightsquigarrow états : $\mathcal{Env}_{\mathfrak{F}} = \mathcal{Env}_{\mathbb{S}\mathbb{P}}$
 - ▶ Σ_{Ev} : signature des évènements
 \rightsquigarrow étiquettes : $\mathcal{L}_{\mathfrak{F}} = T_{\Sigma_{Ev}}^{Query} \times T_{\Sigma_{Ev}}^{Decision}$
- **Système** : $\mathfrak{G} = (\mathfrak{F}, \mathcal{A}x, \delta)$
 - ▶ $\mathfrak{F} = (\mathbb{S}\mathbb{P}, \Sigma_{Ev})$ ($\mathbb{S}\mathbb{P} = (\Sigma, \mathbb{T})$)
 - ▶ $\mathcal{A}x$: ensemble de Σ -formules exprimant les contraintes sur les états initiaux $\mathcal{Env}_0 = \{e \in \mathcal{Env}_{\mathfrak{F}} \mid e \models \mathcal{A}x\}$
 - ▶ $\delta \subseteq \mathcal{Env}_{\mathfrak{F}} \times \mathcal{L}_{\mathfrak{F}} \times \mathcal{Env}_{\mathfrak{F}}$: relation de transition $\Gamma(\mathfrak{G})$: états accessibles
- **LTS** : $(\mathcal{Env}_{\mathfrak{F}}, \mathcal{Env}_0, \mathcal{L}_{\mathfrak{F}}, \delta)$

Exemple : Système BLP

- $\mathcal{G}_{BLP} = (\mathfrak{F}_{BLP}, \mathcal{A}X_{BLP}, \delta_{BLP})$
 - ▶ $\mathfrak{F}_{BLP} = (\mathbb{S}P_{BLP}[Subj, Obj], \Sigma_{Ev}^{BLP})$
 - ★ *Subj* : ensemble de noms de sujets (constantes de sorte *S*)
 - ★ *Obj* : ensemble de noms d'objets (constantes de sorte *O*)
 - ▶ $\mathcal{A}X_{BLP}$: quelconque (selon le domaine d'application considéré)
 - ▶ δ_{BLP} définie comme une fonction de transition :

$$\delta_{BLP}(e, (ask(s, o, a), permit)) = e_{[m(s,o,a)]}$$

$$\delta_{BLP}(e, (release(s, o, a), permit)) = e_{[-m(s,o,a)]}$$

$$\delta_{BLP}(e, (d, deny)) = e$$

- **Politique** : $\wp = (\mathfrak{F}, Rules)$
 - ▶ $\mathfrak{F} = (SP, \Sigma_{Ev})$ ($SP = (\Sigma, T)$)
 - ▶ $Rules \subseteq For(\Sigma) \times \mathcal{L}_{\mathfrak{F}} \times For(\Sigma)$
- **Approche par règles** : $\forall (\psi_{pre}, \gamma, \psi_{post}) \in Rules \quad \psi_{post} = T$
- **Approche par propriétés** : $\forall (\psi_{pre}, \gamma, \psi_{post}) \in Rules \quad \psi_{pre} = T$

Politiques : Propriétés

- \wp est *décidable* : $\forall (\psi_{pre}, \gamma, \psi_{post}) \in \mathcal{Rules}, \forall e \in \mathcal{Env}_{\mathfrak{F}}, e \models \psi_{pre}$ et $e \models \psi_{post}$ sont décidables.
- \wp est *non contradictoire* : $\forall (\psi_{pre}, \gamma, \psi_{post}) \in \mathcal{Rules}, \{\mathbb{T}, \psi_{pre}\}$ et $\{\mathbb{T}, \psi_{post}\}$ sont non contradictoires.
- \wp est *totale à gauche* : $\forall q \in \mathcal{Q}_{Ev} \mathbb{T} \models \bigvee_{\psi \in Pre(q)} \psi$
 $Pre(q) = \{\psi_{pre} \in \mathcal{For}(\Sigma) \mid \exists (d, \psi_{post}) (\psi_{pre}, (q, d), \psi_{post}) \in \mathcal{Rules}\}$
- \wp est *totale à droite* : $\forall q \in \mathcal{Q}_{Ev} \mathbb{T} \models \bigvee_{\psi \in Post(q)} \psi$
 $Post(q) = \{\psi_{post} \in \mathcal{For}(\Sigma) \mid \exists (d, \psi_{pre}) (\psi_{pre}, (q, d), \psi_{post}) \in \mathcal{Rules}\}$
- \wp est *déterministe* : $\forall q \in \mathcal{Q}_{Ev} \forall \psi \neq \psi' \in Pre(q) \{\mathbb{T}, \psi, \psi'\} \models \perp$
- \wp est *fortement totale* : \wp est *totale à gauche* et $\forall q \in \mathcal{Q}_{Ev}$
 $\forall \psi \in Pre(q) \mathbb{T} \models \bigvee_{\psi' \in Post_{\psi}(q)} \psi'$
 $Post_{\psi}(q) = \{\psi_{post} \in \mathcal{For}(\Sigma) \mid \exists d (\psi, (q, d), \psi_{post}) \in \mathcal{Rules}\}$

Exemple : Politique BLP – Approche “règles”

- $\wp_{BLP}^R = (\mathfrak{F}_{BLP}, \mathcal{R}ules_{BLP}^R)$

- ▶ $(\psi_1, (ask(s, o, read), permit), \top) \in \mathcal{R}ules_{BLP}^R$
 $(\neg\psi_1, (ask(s, o, read), deny), \top) \in \mathcal{R}ules_{BLP}^R$

$$\psi_1 = inf(f_o(o), f_s(s)) \wedge [\forall o' m(s, o', write) \Rightarrow inf(f_o(o), f_o(o'))]$$

- ▶ $(\psi_2, (ask(s, o, write), permit), \top) \in \mathcal{R}ules_{BLP}^R$
 $(\neg\psi_2, (ask(s, o, write), deny), \top) \in \mathcal{R}ules_{BLP}^R$

$$\psi_2 = \forall o' m(s, o', read) \Rightarrow inf(f_o(o'), f_o(o))$$

- ▶ $(\psi_3, (release(s, o, a), permit), \top) \in \mathcal{R}ules_{BLP}^R$
 $(\psi_3, (release(s, o, a), deny), \top) \in \mathcal{R}ules_{BLP}^R$

$$\psi_3 = m(s, o, a)$$

Exemple : Politique BLP - Approche “propriétés”

- Confidentialité : “no-read-up”

$$\psi_{MAC} = \forall o, s \ m(s, o, read) \Rightarrow inf(f_o(o), f_s(s))$$

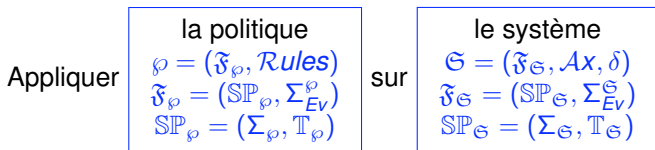
- Confinement : “no-write-down”

$$\psi_{MAC^*} = \forall o_1, o_2, s \ (m(s, o_1, read) \wedge m(s, o_2, write)) \Rightarrow inf(f_o(o_1), f_o(o_2))$$

- $\wp_{BLP}^P = (\mathfrak{F}_{BLP}, Rules_{BLP}^P)$

$$\begin{aligned} (\top, (q, permit), \psi_{MAC} \wedge \psi_{MAC^*}) &\in Rules_{BLP}^P \\ (\top, (q, deny), \neg\psi_{MAC} \vee \neg\psi_{MAC^*}) &\in Rules_{BLP}^P \end{aligned}$$

Appliquer une politique sur un système



- **Condition d'application** : $\mathfrak{F}_\mathfrak{G} \succeq \mathfrak{F}_\varphi$

$$\mathfrak{F}_\mathfrak{G} \succeq \mathfrak{F}_\varphi \Leftrightarrow \Sigma_\mathfrak{G} \supseteq \Sigma_\varphi \wedge \Sigma_{Ev}^\mathfrak{G} \supseteq \Sigma_{Ev}^\varphi \wedge \mathbb{T}_\mathfrak{G} \supseteq \mathbb{T}_\varphi$$

- **Système restreint par une politique** : $\mathfrak{G}|_\varphi = (\mathfrak{F}_\mathfrak{G}, \mathcal{A}\mathcal{X}, \delta_\varphi)$

- ▶ $(e, \gamma, e') \in \delta_\varphi$ ssi $(e, \gamma, e') \in \delta$ et
 - ★ $\gamma \in \mathcal{L}_{\mathfrak{F}_\mathfrak{G}} \setminus \mathcal{L}_{\mathfrak{F}_\varphi}$ ou
 - ★ $\gamma \in \mathcal{L}_{\mathfrak{F}_\varphi}$ et il existe $(\psi_{pre}, \gamma, \psi_{post}) \in \mathcal{R}_\varphi$ tq $e \models \psi_{pre}$ et $e' \models \psi_{post}$

Propriétés garanties par une politique sur un système

- Le système $\mathcal{G} = (\mathfrak{F}, \mathcal{A}x, \delta)$ ($\mathfrak{F} = (\mathbb{S}P, \Sigma_{Ev})$ et $\mathbb{S}P = (\Sigma, \mathbb{T})$) est **correct** vis à vis d'une propriété Ω exprimée par un ensemble de Σ -formules ssi :

$$\forall e \in \mathcal{E}nv_{\mathfrak{F}} \quad e \in \Gamma(\mathcal{G}) \Rightarrow e \models \Omega$$

- Prop.** Si :

- ▶ $\forall e \in \mathcal{E}nv_0 \quad e \models \Omega$ et
- ▶ $\forall (e, \gamma, e') \in \delta \quad e \models \Omega \Rightarrow e' \models \Omega$

alors \mathcal{G} est correct vis à vis de Ω .

- Application.*

- ▶ $\mathcal{G}_{BLP|\varphi_{BLP}^R}$ et $\mathcal{G}_{BLP|\varphi_{BLP}^P}$ sont corrects pour $\{\psi_{MAC}, \psi_{MAC}^*\}$
- ▶ $\Gamma(\mathcal{G}_{BLP|\varphi_{BLP}^R}) = \Gamma(\mathcal{G}_{BLP|\varphi_{BLP}^P})$

Spécifications génériques

- Définir une spécification générique permettant de caractériser un ensemble de propriétés.
- Pour montrer qu'un système garantit une propriété, on construit un morphisme entre les environnements accessibles de ce système et les environnements de la spécification générique.
- *Intérêt* : une même spécification pour plusieurs systèmes différents
 - ▶ *Exemple*. BLP et CW garantissent des propriétés de flots d'information.

Morphisme de signature - Correspondance d'algèbre

● $\Sigma_1 = (\mathcal{S}_1, \mathcal{F}_1, \mathcal{P}_1)$ et $\Sigma_2 = (\mathcal{S}_2, \mathcal{F}_2, \mathcal{P}_2)$

● **Morphisme de signature** $\varphi = (\varphi_S, \varphi_F)$

- ▶ φ_S fonction (totale ou partielle) de \mathcal{S}_1 dans \mathcal{S}_2
- ▶ φ_F fonction (totale ou partielle) de \mathcal{F}_1 dans \mathcal{F}_2 telle que :

$$\forall s_1, \dots, s_n, s \in \text{Dom}(\varphi_S) \quad \forall f : s_1, \dots, s_n \mapsto s \in \text{Dom}(\varphi_F) \\ \varphi_F(f) : \varphi_S(s_1), \dots, \varphi_S(s_n) \mapsto \varphi_S(s) \in \mathcal{F}_2$$

● **Correspondance d'algèbres** : $\tilde{\varphi} = (\varphi, \mapsto)$

- ▶ φ : morphisme de signature
- ▶ $\mapsto \subseteq \text{For}(\Sigma_1) \times \text{For}(\Sigma_2)$ tq $\forall (\psi_1, \psi_2) \in \mapsto, \text{FVar}(\psi_1) = \text{FVar}(\psi_2)$.
- ▶ Relation induite : $\langle \tilde{\varphi} \rangle \subseteq \text{Alg}_{\Sigma_1} \times \text{Alg}_{\Sigma_2}$:

$$(\mathcal{A}_1, \mathcal{A}_2) \in \langle \tilde{\varphi} \rangle \Leftrightarrow \left(\begin{array}{l} \forall (\psi_1, \psi_2) \in \mapsto \quad \forall \sigma : \text{FVar}(\psi_1) \rightarrow A \\ \llbracket \psi_1 \rrbracket_{\mathcal{A}}(\sigma) = \text{true} \Rightarrow \llbracket \psi_2 \rrbracket_{\mathcal{A}'}(\varphi \circ \sigma) = \text{true} \end{array} \right)$$

Exemple : Spécification de Propriétés de flots (1)

- $\mathbb{S}P_{FLOW} = (\Sigma_{FLOW}, \mathbb{T}_{FLOW})$
 - ▶ $\Sigma_{FLOW} = (\mathcal{S}_{FLOW}, \mathcal{F}_{FLOW}, \mathcal{P}_{FLOW})$
 - ★ $\mathcal{S}_{FLOW} = \{Actor, Information\}$
 - ★ \mathcal{F}_{FLOW} quelconque
 - ★ $\mathcal{P}_{FLOW} \supseteq \left\{ \begin{array}{l} Get : Actor, Information, Put : Actor, Information, \\ MoveTo : Information, Information \end{array} \right\}$
 - ▶ $\mathbb{T}_{FLOW} = \left\{ \begin{array}{ll} & MoveTo(o, o) \\ Get(s, o) \wedge Put(s, o') & \Rightarrow MoveTo(o, o') \\ MoveTo(o, o') \wedge Get(s, o') & \Rightarrow Get(s, o) \\ MoveTo(o, o') \wedge Put(s, o) & \Rightarrow Put(s, o') \\ MoveTo(o, o') \wedge MoveTo(o', o'') & \Rightarrow MoveTo(o, o'') \end{array} \right\}$

Exemple : Spécification de Propriétés de flots (2)

- On peut compléter \mathcal{P}_{FLOW} avec :
 - ▶ *Eligible* : Actor, Information
 - ★ Confidentialité : $\psi_{conf} = Get(s, o) \Rightarrow Eligible(s, o)$
 - ▶ *Trustworthy* : Actor, Information
 - ★ Intégrité : $\psi_{int} = Put(s, o) \Rightarrow Trustworthy(s, o)$
 - ▶ *Gflow* : Information, Information
 - ★ Confinement : $\psi_{info} = MoveTo(o, o') \Rightarrow Gflow(o, o')$

Propriétés de flots d'un système

- Système $\mathcal{G} = (\mathfrak{F}, \mathcal{A}x, \delta)$ $(\mathfrak{F} = (\Sigma, \mathbb{T}))$
- Construction d'un morphisme de signature
 - ▶ φ_S
 - ▶ $\mathcal{F}_{FLOW} = \{f : s_1, \dots, s_n \mapsto s \in \mathcal{F}_\Sigma \mid \varphi_S(s) \in \mathcal{S}_{FLOW}\}$
 - ▶ $\varphi_{\mathcal{F}}$ est l'identité
- Définition d'une correspondance $\tilde{\varphi} = (\varphi, \rightsquigarrow)$
- Le système garantit une propriété $\psi \in \mathcal{F}or(\Sigma_{FLOW})$ ssi :

$$\forall e \in \Gamma(\mathcal{G}) \quad \forall e' \in \mathcal{E}nv_{\text{SIP}_{FLOW}} \quad (e, e') \in \langle \tilde{\varphi} \rangle \Rightarrow e' \models \psi$$

Propriétés de flots du système $\mathcal{S}_{|\wp_{BLP}}$

- Morphisme de signature

$$\triangleright \varphi_S(s) = \begin{cases} \text{Information} & \text{si } s = O \\ \text{Actor} & \text{si } s = S \end{cases}$$

- Correspondance $\tilde{\varphi} = (\varphi, \rightsquigarrow)$

$$\rightsquigarrow = \left\{ \begin{array}{ll} (m(s, o, \text{read}), \text{Get}(s, o)), & (m(s, o, \text{write}), \text{Put}(s, o)), \\ (\text{inf}(f_o(o), f_s(s)), \text{Eligible}(s, o)), & (\text{inf}(f_o(o), f_o(o')), \text{Gflow}(o, o')) \end{array} \right\}$$

- BLP garantit la confidentialité et le confinement $\psi = \psi_{\text{conf}} \wedge \psi_{\text{info}}$:

$$\forall e \in \Gamma(\mathcal{S}_{|\wp_{BLP}}) \quad \forall e' \in \mathcal{Env}_{\text{SPFLOW}} \quad (e, e') \in \langle \tilde{\varphi} \rangle \Rightarrow e' \models \psi$$

Conclusion - Travaux futurs

- Cadre permettant de prendre en compte une politique et son environnement
- Cadre permettant de spécifier une politique par des règles ou par des propriétés (flots, ...)
- ↪ Etudier les liens entre approches par règles et approches par propriétés (transformations, équivalences, ...)
- ↪ Implantation Prolog pour des théories sous forme de clauses de Horn
Implantation par de la réécriture ...
- ↪ Cadre de base pour étudier :
 - ▶ la comparaison
 - ▶ la composition