

Gérer la Séparation des Devoirs Dynamique

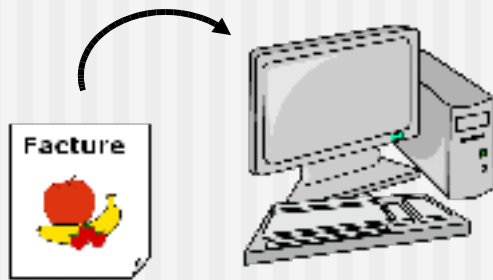
Une extension
temporelle pour RBAC

Sécurité des systèmes d'information
Cours de Stéphane COULONDRE

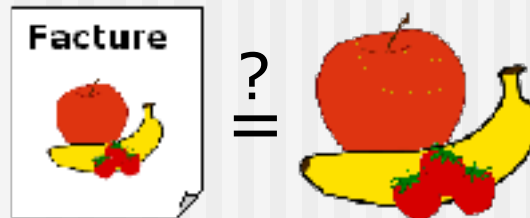
Exposé de Pascal BIHLER (pb@bi-on.de)



Séparation des Devoirs Statique



enregistrer



vérifier



autoriser



Formalisation de RBAC



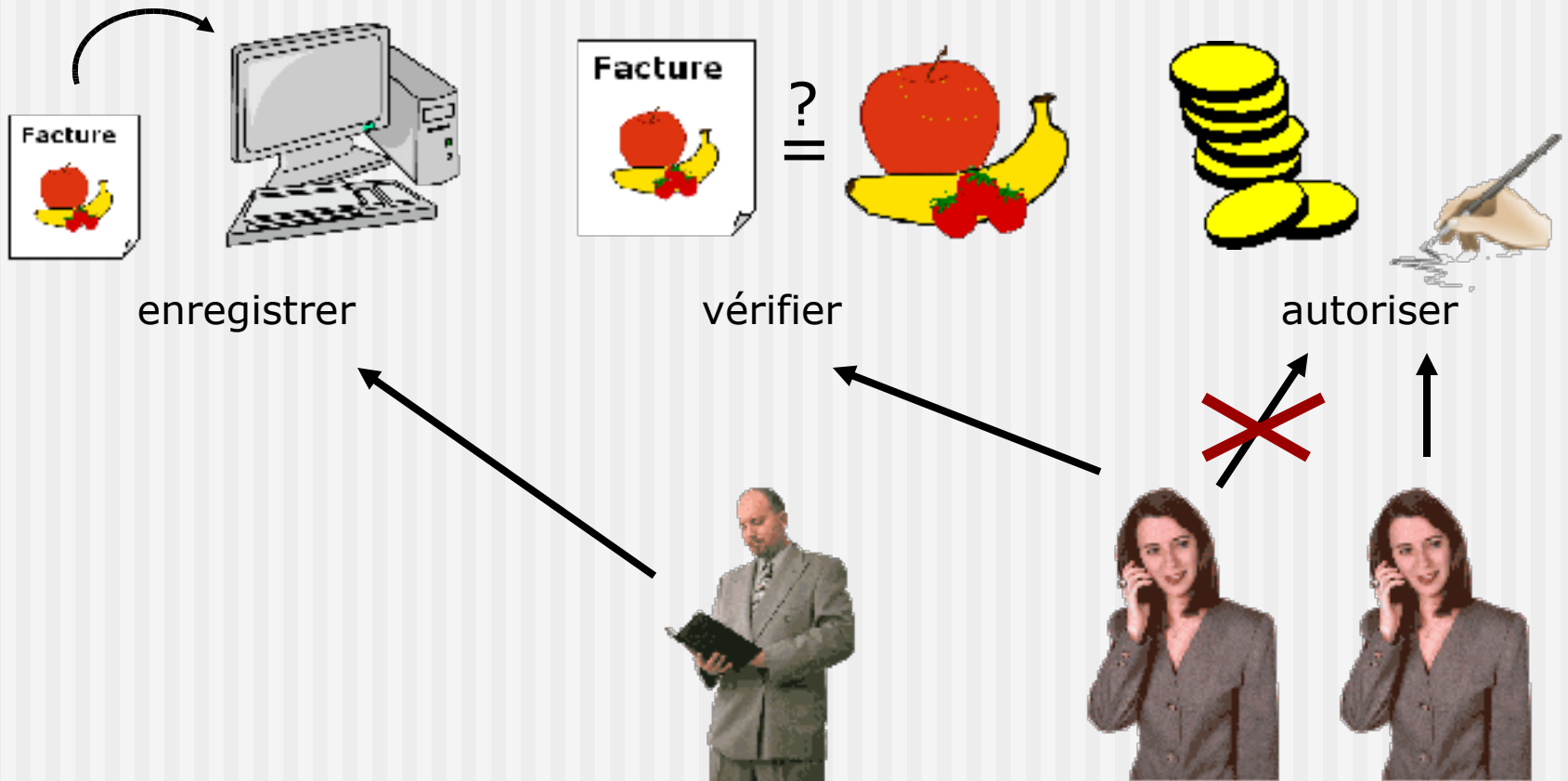
- RBAC en calcul de prédicats (Logique de premier ordre)

```
spec RBAC =  
  sorts Users, Sessions, Roles, Operations, Objects  
  op user: Sessions → Users;  
  preds __assigned_to__: Users × Roles;  
         auth: Roles × Operations × Objects;  
         __active_in__: Roles × Sessions;  
  forall r: Roles; s:Sessions  
    • r active_in s ⇒ user(s) assigned_to r  
end
```

- Exemple: Séparation des devoirs statique(SSoD)

```
pred SSoD ⇔  
  [∀r1, r2: {Roles}; u : Users  
  u assigned_to r1 ∧ u assigned_to r2 ⇒ r1 = r2]
```

Séparation des Devoirs Dynamique



RBAC enrichi

- RBAC avec mémoire d'exécution (« sans état »)

```

spec ExtendedRBAC =
  sorts Users, Sessions, Roles, Operations, Objects
  op user: Sessions → Users;
  preds __assigned_to__: Users × Roles;
          auth: Roles × Operations × Objects;
          __active_in__: Roles × Sessions;

          exec: Sessions × Operations × Objects;

  forall r: Roles; s:Sessions
  • r active_in s ⇒ user(s) assigned_to r

  forall s: Sessions; op: Operations; obj: Objects
  • exec(s,op,obj) ⇒
    ∃r : Roles. r active_in s ∧ auth(r,op,obj)

  end

```

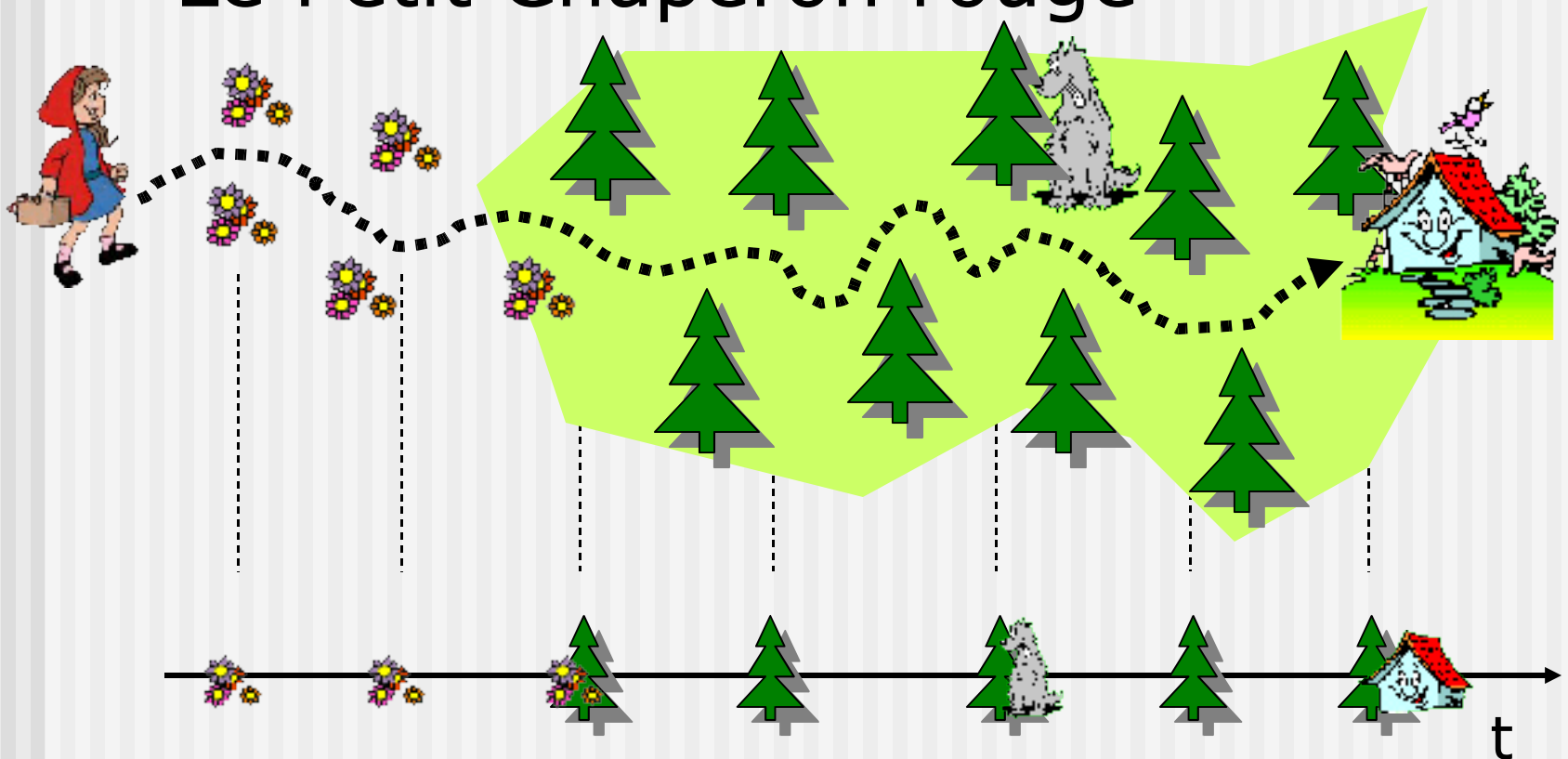
Comparaison des Puissances



	RBAC	ExtendedRBAC
Séparation des devoirs statique (Static Separation of Duties; <i>SSoD</i>)	X	X
Séparation des devoirs dynamique simple (Simple Dynamic Separation of Duties; <i>SDSoD</i>)	X	X
Séparation des devoirs dynamique basée sur objets (Object-Based Dynamic Separation of Duties; <i>ObjDSoD</i>)		X
Séparation des devoirs dynamique opérationnelle (Operational Dynamic Separation of Duties; <i>OpDSoD</i>)		X
Séparation des devoirs dynamique basée sur l'histoire (History-Based Dynamic Separation of Duties; <i>HDSoD</i>)		X

Introduction en Logique Temporelle

■ Le Petit Chaperon rouge



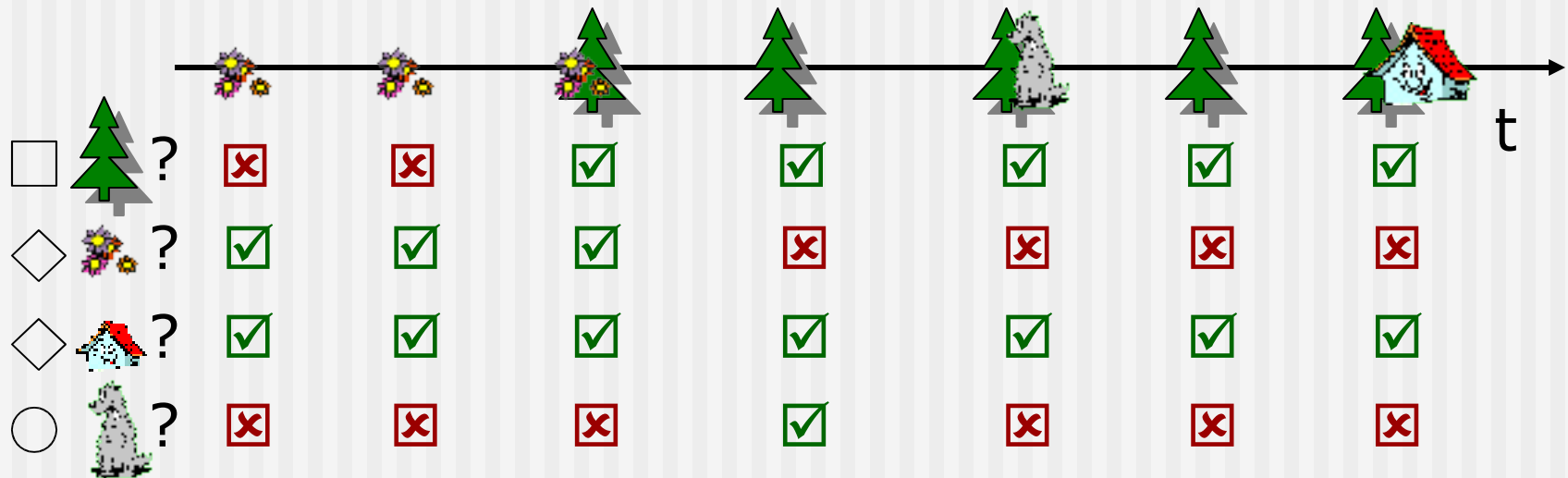
Introduction en Logique Temporelle

- Modalités temporelles:

- toujours en future

- ◇ de temps en temps en future

- dans le prochaine pas



RBAC temporel

■ RBAC avec extension temporelle

```

spec TemporalRBAC =
  sorts Users, Sessions, Roles, Operations, Objects
  rigid op      user: Sessions → Users;
  regid pred auth: Roles × Operations × Objects;
  flexible preds  __assigned_to__: Users × Roles;
                  auth: Users × Operations × Objects;
                  __active_in__: Roles × Sessions;
  forall r: Roles; s:Sessions; op: Operations; obj: Objects
  •  $\square ((\lozenge r \text{ active\_in } s) \Rightarrow \text{user}(s) \text{ assigned\_to } r)$ 
  •  $\square (\text{auth}(u, \text{op}, \text{obj}) \Rightarrow$ 
       $\exists s: \text{Sessions}; r: \text{Roles}.$ 
       $\square (\text{user}(s) = u \wedge r \text{ active\_in } s$ 
       $\wedge \text{auth}(r, \text{op}, \text{obj}))$ 
  •  $(\text{exec}(s, \text{op}, \text{obj}) \Rightarrow \text{auth}(\text{user}(s), \text{op}, \text{obj}))$ 
end

```

Critiques

- ExtendedRBAC simple et puissant
 - mais: Avoir un ensemble des commands exécutés veux dire avoir quand même un état a gérer
- TemporalRBAC complexe
 - Gestion d'état
(comment assure la consistance dans environnements répartis?)
 - « Hypothèse du monde fermé »

Des Questions



Bibliographie

- Till Mossakowski, Michael Drouineaud, Karsten Sohr (2003). *A temporal-logic extension of role-based access control covering dynamic separation of duties*. In Proceedings of the 4th International Conference on Temporal Logic, pp. 83–90. IEEE Computer Society Press.
En ligne: <http://www.tzi.de/~till/papers/RBAC-dyn2.pdf>
- M. Cerioli, T. Mossakowski, H. Reichel (1999). *From total equational to partial first order logic*. In E. Astesiano, H.-J. Kreowski, B. Krieg-Brückner (Eds.), *Algebraic Foundations of Systems Specifications*, pp. 31–104, IFIP State-of-the-Art Reports. Springer Verlag, London.
En ligne: http://www.informatik.uni-bremen.de/~kreo/ifip-WG1.3/ifip_chapters/chapter3.ps
- Wikipedia (2004). *Calcul des prédicats*.
En ligne: http://fr.wikipedia.org/wiki/Calcul_des_pr%C3%A9dicats

Graphiques

- <http://www.openclipart.org>
- http://www.swissfot.ch/0_Iconkids/Geld-1.gif
- <http://vijis.sys.virginia.edu/images/worker.gif>
- http://www.piechdesign.com/About_Us/business_man_1.gif
- http://www.piechdesign.com/Contact_Us/business_woman_on_mobile.gif
- <http://www.mathildegross.de/>
- <http://www.metnitz.at/tourismus/images/haeuschen.gif>
- <http://www.kidsville.de/ameise/quiz/bilder/blumen.gif>
- <http://www.kolumbus.fi/petri.tuomola/illu/clipart/animals/pictures/wolf.gif>