Contrôle d'accès tangible dans les bâtiments intelligents par suivi de flux déclaratifs

François Lesueur, Sabina Surdu, Romuald Thion,
Yann Gripay, Meriam Ben Ghorbel-Talbi

Laboratoire d'InfoRmatique en Image et Systèmes d'information

LIRIS UMR 5205 CNRS/INSA de Lyon/Université Claude Bernard Lyon 1/Université Lumière Lyon 2/École Centrale de Lyon

http://liris.cnrs.fr

Contexte

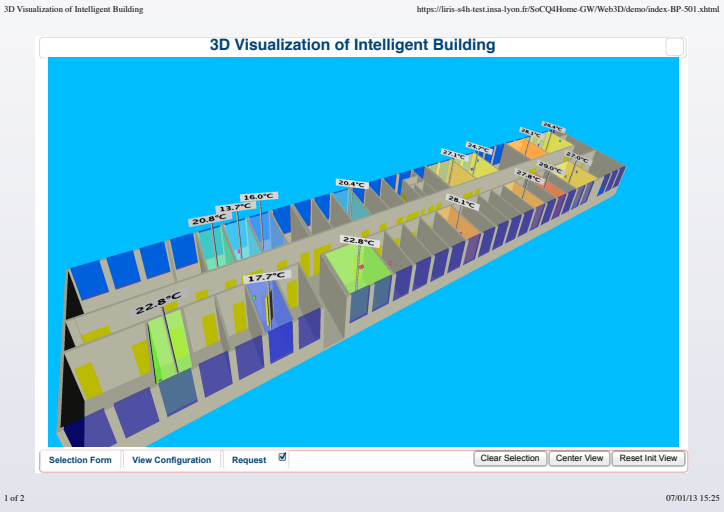
Bâtiment intelligent

- Capteurs : Suivi de l'activité
- Actionneurs : Amélioration de l'environnement (confort, économies)
- Logs

Projet SoCQ4Home

- Plateforme de bâtiment intelligent orientée BD
- Déploiement expérimental dans le bâtiment LIRIS - Blaise Pascal
- 50 capteurs (température, CO_2, présence, etc.)
- 20 pièces équipées

Et concrètement. . .



Une histoire de schtroumpfs...

Ce que l'on souhaite avoir...

- Réglage du chauffage en mode confort basé sur la présence
- Pointage hebdomadaire des heures travaillées
- Audit du comportement du chauffage

...et ce que l'on (peut) souhaite(r) éviter

Que Schtroumpf Curieux ($\neq$ Schtroumpf Root) puisse découvrir :

- S. Paresseux est tellement inactif que son chauffage baisse
- S. Ménager passe très peu de temps dans chaque bureau
- Grand Schtroumpf et la Schtroumpfette font les mêmes horaires tous les mardis

(y compris en analysant l'état des actionneurs/des données internes composées)

TBAC-SoCQ

Motivation

- La (non)-acceptabilité est un frein au déploiement
- Fournir aux usagers un moyen simple, compréhensible, garanti de contrôler la diffusion de *leurs* données
- Tangible, transparent

$\Rightarrow$ Du contrôle pour faciliter le déploiement !

Tuple-Based Access Control (TBAC)

- Contrôle d'accès orienté tuples/BD
- Permissions fixées sur les données initiales (capteurs ici)
- Annotations associées aux tuples à travers tout le système
- Permissions combinées avec la combinaison des tuples
- Contrôle de dissémination d'informations

Plan

État de l'art

Privacy dans les bâtiments intelligents

Solar [Minami & Kotz. 2002]

- ACL sur les événements
- Combinaison des ACL
- Déclassification spécifiée par l'utilisateur, sur un module précis
- Suppose une connaissance et compréhension fine de l'utilisateur, risque de déclassification involontaire

Confab [Hong & Landay. 2004]

- Spécification des droits par les utilisateurs
- Droits indissociables des données
- Pas de traitement des problèmes de combinaison et d'agrégation

Contrôle de flux dans les DSMS

Bell et LaPadula

- Modèle MAC de référence
- Treillis proche de TBAC
- Problème de la déclassification, sans connaître l'historique d'une donnée et ce que voulaient ses sources

Contrôle de dissémination [McCollum, Messing, Notargiacomo. 1990][Sandhu, Ranganathan, Zhang. 2006]

- Contrôle de déclassification
- Règles imposées par les sources de données
- Pas de traitement des problèmes de combinaison à grain fin (granularité document) ni d'agrégation

Contrôle de flux dans les DSMS

Ponctuations de sécurité [Nehme, Rundensteiner, Bertino. 2008]

- Flux de données
- Règles attachées aux tuples et combinées avec les opérations
- Adaptation de modèles existants (RBAC) aux flux
- Pas de modèle de sécurité proposé

SoCQ4Home

SoCQ4Home

SoCQ

- DSMS = Data Stream Management System
- Langage déclaratif SQL-like
- Requêtes continues
- Interaction avec l'environnement concret au travers de services

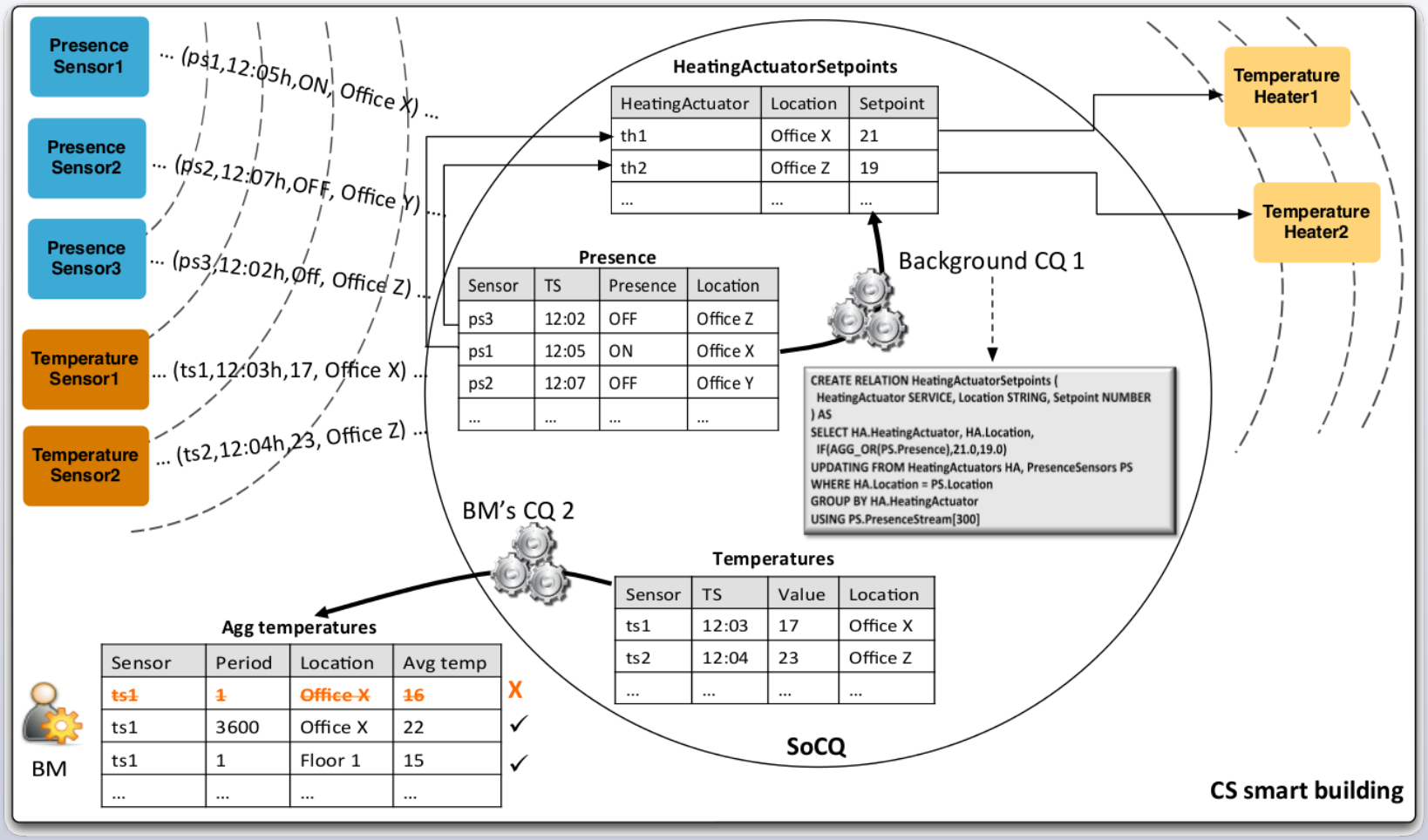
Abstraction relationnelle sur des services distribués

Bâtiment intelligent

- Des services de capteurs/actionneurs
- Un moteur SoCQ

$\Rightarrow$ Programme déclaratif de gestion de bâtiment

Exemple


Presence Sensor1
... (ps1,12:05h,ON, Office X) ...
Presence Sensor2
... (ps2,12:07h,OFF, Office Y) ...
Presence Sensor3
... (ps3,12:02h,Off, Office Z) ...
Temperature Sensor1
... (ts1,12:03h,17, Office X) ...
Temperature Sensor2
... (ts2,12:04h,23, Office Z) ...
HeatingActuatorSetpoints
HeatingActuator | Location | Setpoint
th1 | Office X | 21
th2 | Office Z | 19
... | ... | ...
Presence
Sensor | TS | Presence | Location
ps3 | 12:02 | OFF | Office Z
ps1 | 12:05 | ON | Office X
ps2 | 12:07 | OFF | Office Y
... | ... | ... | ...
Background CQ 1
CREATE RELATION HeatingActuatorSetpoints (
HeatingActuator SERVICE, Location STRING, Setpoint NUMBER
) AS
SELECT HA.HeatingActuator, HA.Location,
IF(AGG_OR(PS.Presence),21.0,19.0)
UPDATING FROM HeatingActuators HA, PresenceSensors PS
WHERE HA.Location = PS.Location
GROUP BY HA.HeatingActuator
USING PS.PresenceStream[300]
Temperature Heater1
Temperature Heater2
BM's CQ 2
Temperatures
Sensor | TS | Value | Location
ts1 | 12:03 | 17 | Office X
ts2 | 12:04 | 23 | Office Z
... | ... | ... | ...
Agg temperatures
Sensor | Period | Location | Avg temp
ts1 | 1 | Office X | 16 X
ts1 | 3600 | Office X | 22 ✓
ts1 | 1 | Floor 1 | 15 ✓
... | ... | ... | ...
BM
SoCQ
CS smart building

Modèle TBAC

Modèle de politique

Principe de base

- Expression uniquement sur les données initiales, donc sur capteurs
- Combinaison automatique des politiques
- Filtre sur les sorties

$\Rightarrow$ Simple, compréhensible, garanti : aspect *tangible*

Semi-anneaux de provenance

Provenance relationnelle

- Dans l'algèbre SPJRU
- L'algèbre respecte les propriétés d'un semi-anneau
- Les annotations doivent respecter cette structure pour "bien se combiner"

Semi-anneau d'annotations

- Un ensemble K des annotations
- $(K, \oplus, 0)$ est un monoïde commutatif
- $(K, \otimes, 1)$ est un monoïde
- $\otimes$ est distributif pour $\oplus$
- 0 est absorbant pour $\otimes$

Pour le contrôle de flux

Définir l'ensemble K des droits

Qu'est-ce qu'un droit élémentaire ?

Définir les opérations $\oplus$ et $\otimes$

Comment combiner des droits vers un nouveau droit de K ?

- $\otimes$ matérialise l'utilisation conjointe des entrées (jointure)
- $\oplus$ matérialise l'utilisation alternative des entrées (sélection, projection, union)

Définir la fonction de décision

Comment décider si l'accès à un tuple annoté est autorisé ?

SmartBuilding-TBAC

Définir la structure des annotations

Annotation de chaque tuple

$K = \mathcal{P}((\perp + Prerequis) \times \mathcal{P}(Users))$

Prérequis

$Prerequis = (T \times S \times OP)$

- T : niveau d'agrégation temporelle
- S : niveau d'agrégation spatiale
- OP : opération d'agrégation

Exemple

$k = \{((week, office, sum), \{S.Lunettes, S.Grognon\}),$
$(\quad (\perp) \quad , \quad \{Schtroumpfette\} \quad)\}$

Agrégation des flux 1/2

Problème

- Soit le flux suivant en entrée du système (présence)
  - $4h17; 13h18\{((day, office, sum), \{S.Lunettes, S.Grognon\})\}$
  - $3h35; 18h25\{((day, office, sum), \{S.Lunettes, S.Grognon\})\}$
- S. Lunettes ne doit pouvoir accéder qu'à l'agrégat journalier

Comment valider l'agrégation ?

- À la sortie du système ?
  - "SFW Timestamp=18h24", "18h25", *etc.*
  - 1 seule valeur, l'agrégation en sortie ne sert plus à rien
  - Nécessiterait d'utiliser des *critères* sur la forme de la sortie autorisée
- À l'entrée du système ?
  - Duplication pour chaque niveau d'agrégation
  - Requêtes doivent être exprimées sur les bons niveaux d'agrégation (étudié dans le domaine des entrepôts)

Annotations internes

Annotation de chaque tuple

$K = \mathcal{P}(Users)$

Exemple

$Stream3452 : \{((week, office, sum), \{Lunettes, Grognon\}),$
$(\quad (\perp) \quad , \quad \{Schtroumpfette\} \ )\}$
$\rightarrow Stream3452\_Week\_Office\_Sum : \{Lunettes, Grognon\}$
$\rightarrow Stream3452\_Raw : \{Schtroumpfette\}$

Définir les opérations : $\otimes$

$\otimes$ pour les utilisations conjointes

- $\cap$: intersection d'ensembles d'utilisateurs
- $\{Lunettes, Grognon\} \otimes \{Lunettes, Farceur\} = \{Lunettes\}$

Exemple

Loc	Pres	stag
Off X	True	$\{Lunettes, Grognon\}$
Off Y	True	$\{Grognon\}$

Loc	Temp	stag
Off X	27	$\{Lunettes, Farceur\}$
Off Y	15	$\{Grognon\}$

Jointure sur Loc :

Loc	Pres	Temp	stag
Off X	True	27	$\{Lunettes\}$
Off Y	True	15	$\{Grognon\}$

Définir les opérations : $\oplus$

$\oplus$ pour les utilisations alternatives

- $\cup$: union d'ensembles d'utilisateurs
- $\{Lunettes, Grognon\} \oplus \{Farceur\} = \{Lunettes, Grognon, Farceur\}$

Exemple

Loc	Pres	stag
Off X	True	$\{Lunettes, Grognon\}$
Off Y	True	$\{Farceur\}$

Loc	Build	stag
Off X	A	*Users*
Off Y	A	*Users*

Jointure sur Loc puis Projection :

Build	Pres	stag
A	True	$\{Lunettes, Grognon, Farceur\}$

Définir la fonction de décision

Résultat d'une requête de $u \in U$

- Pour chaque tuple t annoté k, t doit être visible ssi $u \in k$

Exemple

Loc	Pres	stag
Off X	True	$\{Lunettes, Grognon\}$
Off Y	True	$\{Grognon\}$

Vue de Lunettes :

Loc	Pres	stag
Off X	True	$\{Lunettes, Grognon\}$

Vue de Grognon :

Loc	Pres	stag
Off X	True	$\{Lunettes, Grognon\}$
Off Y	True	$\{Grognon\}$

Ce que nous dit la provenance

Sommes-nous dans le bon cadre ?

- $(\mathcal{P}(U), \cup, \emptyset)$ est un monoïde commutatif
- $(\mathcal{P}(U), \cap, U)$ est un monoïde
- $\cap$ est distributif sur $\cup$
- $\emptyset$ est absorbant pour $\cap$

Et donc

- Combinaison compatible avec l'algèbre relationnelle
- Filtre au début/à la fin équivalent
- Respect des politiques initiales lors de l'accès à des données composées

Administration

Démarche

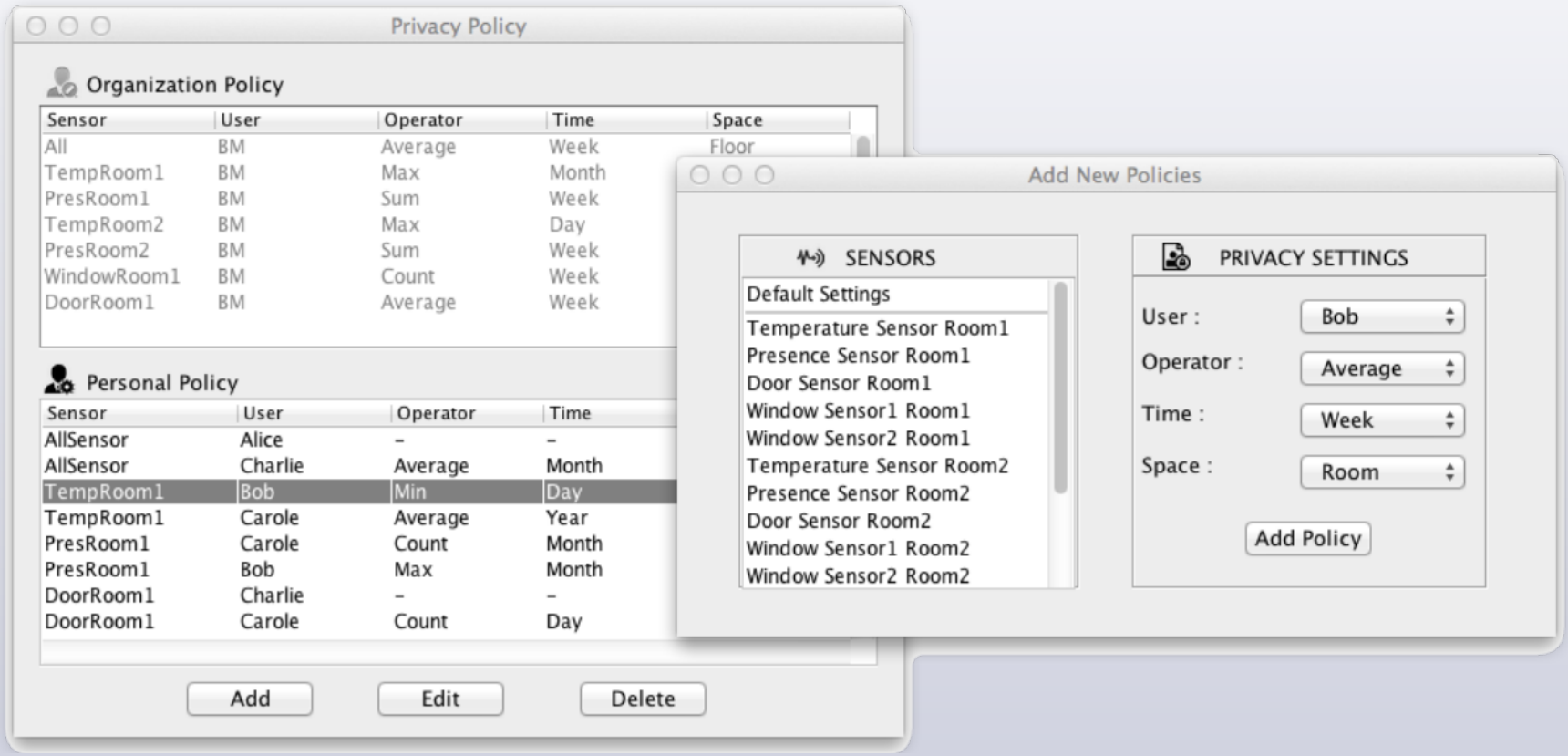
Politique fixée sur les capteurs

- Chaque capteur est associé à des utilisateurs
- Ces utilisateurs posent les contrôles sur les données issues de ce capteur
- Les différents critères sont combinés ($\otimes$)

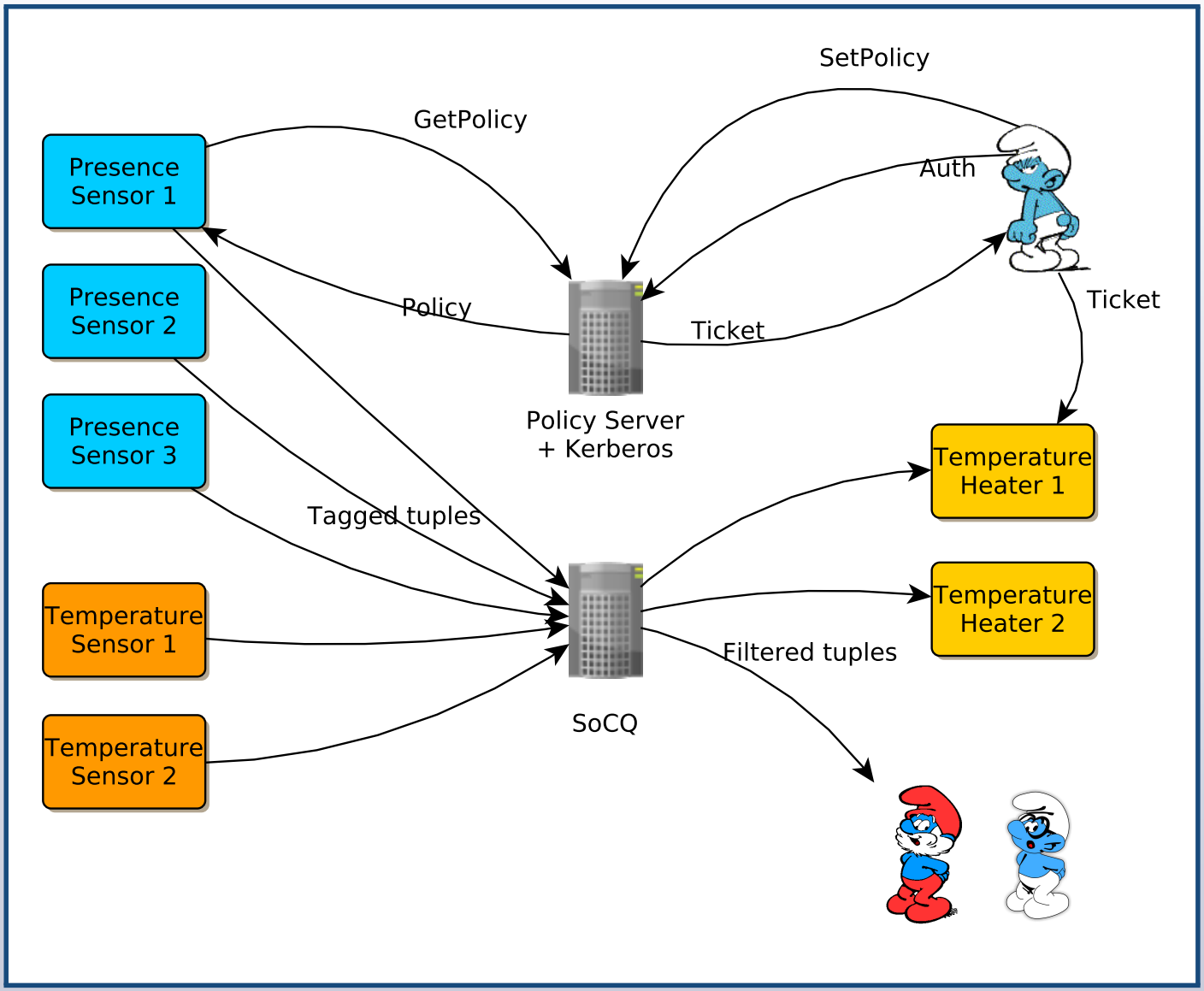
Squelette de l'organisation

- La spécification manuelle peut être fastidieuse
- L'organisation fournit un squelette, modifiable ou non
- Transparent

Interface de saisie de la politique



Prototype en cours de réalisation



Conclusion

Approche TBAC-SoCQ

- Gestion déclarative du bâtiment
- Suivi de flux déclaratifs
- Langage algébrique
- Garanties, aspect *tangible*

→ Intégration de déclassifications à BLP

Caractéristiques

- Suivi de flux relationnels : beaucoup plus simple que l'impératif ! (pas de conditionnelle, de boucles, de variables, etc.)
- Grain fin, ce qui est propagé a réellement été utilisé
- Application bâtiment présentée : on peut faire des programmes complexes en relationnel

Perspectives

Prototypage (en cours)

- Instrumentation du moteur SoCQ (10 opérateurs)
- Évolution du protocole de communication Ubiware (négociation, enrichissement, filtrage)
- Intégration du serveur de politiques + Kerberos (administration centralisée et authentification)

Modèle de contrôle

- Remplacer l'agrégation en entrée par des propriétés en sortie, tout en conservant l'aspect compréhensible
- Gérer le masquage de tuples par d'autres plus confidentiels (langage algébrique)
- Découvrir les canaux environnementaux
- Des politiques plus complexes pour d'autres utilisations

Contrôle d'accès tangible dans les bâtiments intelligents par suivi de flux déclaratifs

François Lesueur, Sabina Surdu, Romuald Thion,
Yann Gripay, Meriam Ben Ghorbel-Talbi

Laboratoire d'InfoRmatique en Image et Systèmes d'information

LIRIS UMR 5205 CNRS/INSA de Lyon/Université Claude Bernard Lyon 1/Université Lumière Lyon 2/École Centrale de Lyon

http://liris.cnrs.fr