Projet Modélisation de Logiciel Surs
Etude du contrôle d'accès au Gloria

Pierre Maeckereel (LE)
Rémi Morel (LE)
Yannick Philippe (IL)
Matthieu Rapenne (IL)

15 décembre 2017

1 Sujet

Un laboratoire célèbre GLORIA développe des recherches top secrètes et hautement sensibles. Cette situation lui impose de contrôler l'accès de ses visiteurs et de ses employés. Pour cela, il dispose d'une brigade d'hôtesses qui peuvent, après vérification de l'identité d'un visiteur ou autre, donner un accès au bâtiment du GLORIA. Un second accès se fait par un mécanisme d'identification fiable permettant à une personne accréditée d'accéder au bâtiment. Le mécanisme d'identification automatique peut faire appel à des saisies d'empreintes ou à des mécanismes de sécurité maximale. On a donc plusieurs protocoles possibles :

- Une personne A vient visiter une personne B, l'hôtesse enregistre l'identité du visiteur, lui donne des papiers de visite et l'accès au bâtiment s'il est autorisé.
- Une personne A a une carte d'accès et l'utilise lors de son arrivée ; si l'accès lui est accordée, alors le dispositif d'accès est ouvert et la personne A peut entrer dans le bâtiment.
- Une personne A veut sortir du bâtiment et l'hôtesse est présente ; l'hôtesse enregistre la sortie de cette personne qui sort du bâtiment.
- Une personne A veut sortir du bâtiment et l'hôtesse n'est plus présente ; A doit indiquer un code sur un dispositif contrôlant la sortie.
- Une personne A a un accès par carte et doit présenter cette carte pour avoir l'autorisation de sortir.

Dans la mesure où une personne peut perdre son accès quand elle est dans le bâtiment, il faut prévoir un numéro d'appel de la sécurité assurée à distance 24/24. En cas d'urgence, les dispositifs de sécurité libèrent tous les accès pour

garantir la sûreté des personnes.
Les droits d'accès des personnes dépendent de leur catégorie et selon celle-ci, cette personne est autorisée à entrer au laboratoire à certains moments de la journée, lors des jours ouvrés. Personne n'est autorisé à entrer au laboratoire avant 7h00 du matin et après 22h00. Le laboratoire comprend deux types de personnes : les permanents et les non-permanents. Un non-permanent n'a pas le droit d'entrer après 18h00 et avant 8h00 du matin et un non-permanent n'a pas le droit d'entrer au laboratoire le samedi, le dimanche ou pendant un jour férié. Quand le laboratoire est fermé, personne ne peut y pénétrer. Il est fermé à certaines dates définies par la maintenance.

Dans ce projet, nous devrons donc :

- Développer une suite de modèles par raffinement en expliquant pour chaque étape les choix faits et comment ils peuvent être justifiés.
- A partir du modèle précédent, écrire un petit programme prototypant ce modèle.

2 Définition du modèle

D'après l'énoncé ci-dessus, il est important de définir les différents éléments de base qui vont composer notre modèle.

Ainsi, si nous analysons le problème de manière très globale, nous avons des personnes qui peuvent être ou non dans un bâtiment, ce qui se traduit par la définition de la localisation desdites personnes.

2.1 Définition des personnes

Le laboratoire du GLORIA ayant du personnel et des visiteurs, il faut pouvoir modéliser et savoir quel type de personne est à l'intérieur ou en dehors du bâtiment. C'est pour cela que sur l'ensemble des personnes, nous avons les personnes présentes à l'intérieur et celles à l'extérieur.
Soit **P** l'ensemble des personnes, **PE** l'ensemble des personnes présentes à l'extérieur, et **PI** l'ensemble des personnes présentes à l'intérieur. Alors : $P = PE \cup PI$

Contraintes : Maintenant ces personnes peuvent être soit à l'intérieur, soit à l'extérieur du laboratoire, mais pas les deux à la fois. Ce qui implique que pour chaque personne :
$\forall p \in P, (p \in PE \wedge p \notin PI) \vee (p \in PI \wedge p \notin PE)$

3 Raffinement

Maintenant que le modèle est définit de manière très générale , nous allons le raffiner et lui rajouter des contraintes.

3.1 Types de personne

On sait que les personnes du modèle peuvent être de deux types, des personnes externes au laboratoire **PExt** et des personnes travaillant pour le laboratoire **PLab**. $P = PExt \cup PLab$

Contrainte: Ce qui implique que chaque personne est soit **PExt** soit **PLab** mais pas les deux:
$\forall p \in P, (p \in PExt \wedge p \notin PLab) \vee (p \in PLab \wedge p \notin PExt)$

Note: Nous pouvons donc dire que si :
$P = PE \cup PI$
$P = PExt \cup PLab$
et que :
$PE = (PExt \cup PLab) \notin PI$
$PI = (PExt \cup PLab) \notin PE$
alors nous pouvont définir l'ensemble **P** avec **PI**, **PE**, **Pext**, **PLab** telle que:
$P = ((PExt \cup PLab) \notin PE) \cup ((PExt \cup PLab) \notin PI)$

3.2 Personne du laboratoire

Le personnel du laboratoire disposant de droit en fonction de leur statut (permanent ou non), il est nécessaire de connaître les listes de ces personnes.

C'est pourquoi nous avons un ensemble **PLab** du Personnel au GLORIA, décomposé en Personne Permanante **PP** et Personne non Permanante **PNP**. De telle sorte que : $PLab = PP \cup PNP$

Contrainte : On peut noter qu'une personne permanente n'est pas non permanente et inversement ce qui se traduit par :
$\forall p \in PLab, (p \in PP \wedge p \notin PNP) \vee (p \in PNP \wedge p \notin PP)$

3.3 Personne extérieure

Les personnes extérieures pouvant venir visiter le laboratoire, il faut savoir quelle personne extérieure est dans le le laboratoire à un moment donné.

C'est pourquoi **PExt** est composé des personnes ayant une autorisation **PAut** et les personnes n'ayant pas d'autorisation **PNAut**
De telle sorte que : $PExt = PAut \cup PNAut$

Contrainte : On peut noter qu'une personne extérieure ne peut pas être autorisée et non autorisée en même temps ce qui se traduit par :
$\forall p \in PExt, (p \in PAut \wedge p \notin PNAut) \vee (p \in PNAut \wedge p \notin PAut)$

3.4 Horaire, Date et Maintenance

Le laboratoire secret du GLORIA étant très réglementé, il est nécessaire de définir des variables qui serviront à modéliser l'horaire durant lequel la simulation se trouve, si la date est un jour ouvré ou non et si l'établissement est en maintenance. $H \in N$

Nous aurons donc 3 variables :

- Une variable horaire **H**, compris entre 00h00 et 23h59
- Une variable de jour ouvré **JO** qui nous indique si nous sommes un jour différent de samedi , dimanche ou férié
- Une variable de maintenance **M** qui nous indique si le laboratoire est en maintenance

avec ces trois variables, nous pouvons donc raffiner le modèle avec les contraintes suivantes.

$((H \leq 7 \vee H \geq 22) \vee \neg JO \vee M) \Rightarrow PI = \emptyset$
$((H \geq 7 \wedge H \leq 8) \vee (H \geq 18 \wedge H \leq 22)) \vee JO \vee \neg M) \Rightarrow (\forall p, p \in Plab \wedge p \in PI \Rightarrow p \in PP)$

3.5 Accès au bâtiment

Le GLORIA devant gérer des visiteurs et le personnel du laboratoire, il est nécessaire d'avoir un système qui permette de contrôler les flux des personnes.

Pour nous aider nous aurons 2 variables :

- Une variable hôtesse **Hot** qui indique si une hôtesse et présente à l'accueil du GLORIA et va donc gérer les flux pour les visiteurs
- Une variable sécurité **S** qui indique si le bâtiment est en alerte et qui permet de sortir du bâtiment en securité si il y a un problème

Ainsi ces variables permettent de réaliser les actions de passage dans le bâtiment et de sortie du bâtiment.

3.5.1 Visiteur

Si **S** est actif : on déverrouille les sorties de secours.
On passe les visiteurs de **PI** $\rightarrow$ **PE** et de **PAut** $\rightarrow$ **PNAut**

Si un visiteur veut passer de **PE** $\rightarrow$ **PI** et que **Hot** est vraie : il rempli un papier à l'accueil
On passe le visiteur de **PE** $\rightarrow$ **PI** et de **PNAut** $\rightarrow$ **PAut**

Si un visiteur veut passer de **PI** $\rightarrow$ **PE** et qui sont dans **PAut** et **Hot**: on rend sa carte au visiteur
On passe de **PI** $\rightarrow$ **PE** et de **PAut** $\rightarrow$ **PNAut**

Si un visiteur est dans **PI** mais est dans **PNAut**: il appelle le service 24h/24
On passe de **PI** $\rightarrow$ **PE**

Nous pouvons aussi ajouter des actions pour que le visiteur soit sorti du bâtiment si un certain horaire est dépassé et ajouter la variable Horaire à l'action d'entrer dans le bâtiment pour restreindre l'accès aux heures indiquées.

3.5.2 Personnel

Si **S** est actif : on déverrouille les sorties de secours
On passe le chercheur de **PI** $\rightarrow$ **PE**

Si un chercheur veut passer de **PE** $\rightarrow$ **PI**: on ouvre la porte
On passe du chercheur de **PE** $\rightarrow$ **PI**

Si un chercheur veut passer de **PI** $\rightarrow$ **PE** et que **Hot** est vraie : il peut sortir par la porte
On passe le chercheur de **PI** $\rightarrow$ **PE**

Si un chercheur veut passer de **PI** $\rightarrow$ **PE** et que **Hot** n'est pas vraie : il doit saisir un code
On passe le chercheur de **PI** $\rightarrow$ **PE**

Nous pouvons aussi ajouter des actions pour que le chercheur soit sorti du bâtiment si un certain horaire est dépassé (en fonction de si il sont permanents) et ajouter la variable horaire à l'action d'entrer dans le bâtiment pour restreindre l'accès aux heures indiquées.

4 Propriétés de sûreté

- Une personne accède au laboratoire entre 7h00 et 22h00
- PI est vide entre 22h00 et 7h00
- Un visiteur autorisé ne peut être à l'extérieur
- Une personne extérieure ne peut accéder au laboratoire si sa carte d'accès a été refusée.