M2-TIW4 sécurité des systèmes d'informations
Contrôle continu final – 1h30

Master 2 *Technologie de l'Information (TI)*
Promotion 2012 – 2013

Tous les documents papiers sont autorisés. Le barème est indicatif. La rigueur, la clarté, la pertinence et la concision des réponses font partie intégrante des critères d'évaluation.

Exercice 1 : modèles mandataires à niveaux (/8)

Les modèles mandataires à niveaux font l'hypothèse que les niveaux de sécurité disposent d'une structure *d'ordre partiel*, c'est-à-dire que l'ensemble L des niveaux est muni d'une relation $\leq_L \subseteq L \times L$ transitive [1], réflexive [2] et antisymétrique [3].

On note S l'ensemble des sujets du système et O celui des objets. À chaque sujet et à chaque objet est associé un unique niveau de sécurité, formellement [4] [5] $cl : S \to L$ et $la : O \to L$. On désigne par $M \subseteq S \times \{r, w\} \times O$ l'ensemble des autorisations du système pour S, O, cl et la fixés. Les modèles à niveaux utilisent deux règles pour dériver les autorisations :

- $(s, r, o) \in M$ si et seulement si $la(o) \leq_L cl(s)$
- $(s, w, o) \in M$ si et seulement si $cl(s) \leq_L la(o)$

1. Calculer la matrice d'accès $M \subseteq \{a, b, c\} \times \{r, w\} \times \{1, 2, 3, 4\}$ obtenue avec :
   - $L = \{pub, conf, secret, top\}$ totalement ordonné $pub \leq_L conf \leq_L secret \leq_L top$
   - la fonction cl telle que $cl(a) = pub, cl(b) = secret, cl(c) = conf$
   - la fonction la telle que $la(1) = top, la(2) = pub, la(3) = secret, la(4) = pub$
2. Une matrice M non-vide peut-elle toujours être obtenue à partir d'un modèle à niveau ? Si oui, le prouver, sinon produire un contre-exemple.
3. Prouver que si un utilisateur peut lire un fichier o, et qu'il peut écrire dans un autre fichier o', alors le label de o' est supérieur à celui de o. Commenter cette propriété en terme de fuite d'information.
4. On aimerait imposer dans la politique de sécurité que certains documents sensibles soient signés par un supérieur disposant d'une accréditation supérieure à celle du rédacteur principal. Est-ce possible dans un modèle mandataire ? Justifier.
5. On considère l'ordre partiel des parties de $\{compta, inge\}$ muni de l'inclusion $\subseteq$ entre parties. Dessiner l'ordre partiel produit en combinant celui-ci avec L défini précédemment.
6. Définir la règle de lecture sur la structure $\wp(\{compta, inge\}) \times L$ des niveaux de sécurité obtenue à la question précédente.

1. $\forall a, b, c. a \leq_L b \wedge b \leq_L c \Rightarrow a \leq_L c$
2. $\forall a. a \leq_L a$
3. $\forall a, b. a \leq_L b \wedge b \leq_L a \Rightarrow a = b$
4. cl pour *clearance*, l'accréditation de l'utilisateur
5. la pour le *label* de l'objet

Exercice 2 : modèles à rôles (/6)

Pour les collections U d'utilisateurs, P de permissions et R de rôles, on donne les relations $Ura \subseteq U \times R$ et $Pra \subseteq R \times P$ d'une politique RBAC ci-dessous. On note les permissions sous la forme $ao \in P$ où a est une action et o un objet.

	I	M	P	S
Alice	×	×		×
Bob		×		
Charly	×		×	×
Denise	×			×

	r1	w1	r2	w2	r3	w3
I	×		×		×	
M		×	×	×		
P						×
S	×		×			

1. Calculer la matrice des droits $M \subseteq U \times P$ à partir des relations Ura et Pra.
2. Réorganiser les rôles en une nouvelle hiérarchie de quatre rôles *qui utilise l'héritage* et dans laquelle chaque utilisateur et chaque permission sont associés à *exactement* un seul rôle. Préciser les utilisateurs et les permissions affectés à chaque rôle.
3. On autorise désormais un utilisateur à être affecté à plusieurs rôles simultanément. Modifier la hiérarchie et les affectations de la question précédente pour réduire le nombre de rôles. Commenter l'intérêt de la hiérarchisation des rôles et de l'affectation multiple sur cet exemple.
4. On souhaite ajouter la contrainte de séparation des tâches « *il est interdit de pouvoir écrire à la fois dans 1 (`w1`) et dans 3 (`w3`)* ». Avec une relation d'exclusion mutuelle binaire entre rôles, exprimer cette contrainte sur les rôles originaux.
5. On s'intéresse à une variante de l'exclusion mutuelle dans laquelle on ne souhaite pas interdire qu'un *utilisateur* soit membre de deux rôles en exclusion mais qu'aucune *permission* ne soit commune à deux rôles en exclusion. Donner la collection exhaustive des contraintes de ce type qui peuvent être supposées pour la relation Pra donnée.

Exercice 3 : modélisation avec les rôles (/6)

On considère une structure composée d'équipes. Une équipe est soit une équipe fonctionnelle soit une équipe transverse. Un acteur de la structure ne peut appartenir qu'à une seule équipe fonctionnelle mais à plusieurs équipes transverses. Chaque équipe fonctionnelle a ses propres applications de gestion auxquelles tous les membres de l'équipe ont accès. Chaque équipe a au moins une application de gestion propre. Les équipes fonctionnelles sont divisées en deux secteurs A et B. Toutes les équipes d'un secteur ont un ensemble d'applications en commun. Parmi les acteurs, on distingue trois profils *responsable*, $administratif$ et *camarade*. Le profil $administratif$ n'est pas compatible avec les deux autres. Il ne peut y avoir qu'un seul *responsable* par équipe, le nombre de *camarade*s n'est pas limité.

On considère la collection d'utilisateurs $U = \{u_0^1 \dots u_{n_1}^1, \dots, u_0^p \dots u_{n_p}^p\}$ et la collection $E = \{e_0 \dots e_p\}$ d'équipes. Les équipes d'indices pairs (e_0, e_2 etc.) sont celles du secteur A et celles d'indices impairs celles du secteur B. Les utilisateurs u_n^i sont ceux de l'équipe i, u_0^i étant le responsable de l'équipe i en question. Dans le cas des équipes du secteur B, c'est l'utilisateur u_1^i qui est administratif. Les applications de gestions sont identifiées par des entiers.

1. Modéliser le plus rigoureusement possible cette structure dans un système RBAC avec rôles hiérarchisés et contraintes d'exclusion mutuelle, en l'illustrant avec une petite valeur de p, quelques utilisateurs et quelques applications.
2. Quelles sont les contraintes de ce texte que vous ne pouvez pas prendre en compte avec le système RBAC de la question précédente. Quelle(s) extension(s) faudrait-il proposer pour pouvoir les intégrer ?

Exercice 4 : commentaire d'une actualité (/2)

Extrait [6] de l'article « *Adoption of Traffic Sniffing Standard Fans WCIT Flames* » [7], relayé en France sous le titre « *L'ITU et le DPI : ça va être dur d'expliquer ça à ma grand-mère* » [8].

> *The telecommunications standards arm of the U.N. has quietly endorsed the standardization of technologies that could give governments and companies the ability to sift through all of an Internet user's traffic [...]. At the core of this development is the adoption of a proposed international standard that outlines requirements for a technology known as "Deep Packet Inspection" (DPI). As we've noted several times before, depending on how it is used, DPI has the potential to be extremely privacy-invasive, to defy user expectations, and to facilitate wiretapping.*
>
> *The adoption of this standard, officially known as "Requirements for Deep Packet Inspection in Next Generation Networks," or "Y.2770" came to light last week during the World Telecommunication Standardization Assembly (WTSA), an international meeting held every four years in which the standards-setting body of the U.N.'s International Telecommunication Union, known as the ITU-T, charts the course of its work.*

Cité depuis Wikipedia "*DPI is a form of computer network packet filtering that examines the data part (and possibly also the header) of a packet as it passes an inspection point*".

1. À la lumière des connaissances acquises, expliquer ce que cette technologie apporte vis-à-vis des techniques de filtrage de paquets classiques des pare-feux statiques et dynamiques. Expliquer et commenter brièvement quelles peuvent être ses applications pour la sécurité ainsi que les dangers de telles technologies vis-à-vis de la protection de la vie privée.

6. *to sift* : examiner, *wiretapping* : écoutes téléphoniques, *to chart* : planifier

7. `https://www.cdt.org/blogs/cdt/2811adoption-traffic-sniffing-standard-fans-wcit-flames`, 28 novembre 2012

8. `http://reflets.info/l-itu-et-le-dpi-ca-va-etre-dur-dexpliquer-ca-a-ma-grand-mere/`, 6 décembre 2012