# IFT6271–Sécurité Informatique
# (Devoir #3, Hiver 2014)

Louis Salvail[1]

Université de Montréal (DIRO), QC, Canada
salvail@iro.umontreal.ca
Bureau: Pavillon André-Aisenstadt, #3369

## 1 Mise en place

Répondez **très clairement** aux questions suivantes. Tâchez d'être concis. Lisez le scénario en détails avant de vous lancer. La date de remise est le jeudi 17 avril 2014, 17:30. La correction du devoir aura lieu à 17:30 jeudi le 17 avril. L'examen final est jeudi le 24 avril 2014, 17:30, Z-215. Tout retard pour la remise du devoir sera refusé.

## 2 Services Secrets

Le service secret de Transylvanie (SST) a plusieurs agents qui sont bien souvent en déplacement. Les agents se déplacent avec leur ordinateur portable. Le SST veut mettre en ligne un service de dépôt de documents pour permettre àl'information de circuler dans le SST, tout en respectant la classification des documents. Chaque agent connaît le classification de sécurité des documents sur lesquels elle/il travaille. Les classifications possibles pour la sécurité d'un document sont: $C = \{\texttt{public}, \texttt{secret}, \texttt{top}-\texttt{secret}\}$. Chaque employé du SST possède également une classification de sécurité indiquant son droit pour la lecture de documents. Un employé avec classification $\texttt{top}-\texttt{secret}$ peut lire n'importe quel document, un employé avec classification `secret` peut lire les documents `public` et `secret` tandis qu'un employé avec classification `public` ne peut lire que les documents `public`. Notez que la classification `public` ne veut pas dire que n'importe qui peut lire le document mais plutôt que tous les employés du SST peuvent le lire.

Le SST veut donc mettre en place des serveurs responsables pour ranger les documents des agents en déplacement. Ces serveurs permettent aux agents d'y déposer un document avec une certaine classification. Seuls les employés du SST avec au moins cette classification peuvent lire le document. Le serveur devrait également assurer l'intégrité des documents qu'il contient. Autrement, le serveur se comporte comme une **Dropbox**. Il s'agit d'un service de stockage et de partage de copies de documents en ligne. Le SST veut que le service de stockage et de partage ne permettent pas d'apprendre la teneur d'un document même si l'authentifiant d'un employé est obtenu. C'est-à-dire qu'il n'est pas possible, même à un adversaire externe au SST qui "*devine*" l'authentifiant d'un employé, de lire ou de déposer un document, même de classication `public`. Le SST veut également un système qui soit tel que même si le serveur est sous le contrôle d'un adversaire externe au SST (par exemple, un agent du service secret de Poldévie), il n'est pas possible de lire les documents qui y sont déposés pas plus que d'y déposer des documents frauduleux sans qu'ils ne puissent être détectés comme tel.

Votre mission est d'élaborer des politiques de sécurité pour les usagers du système ainsi que pour les techniciens responsables pour la mise en place des serveurs.

## 3 Les Questions

Je vous demande de faire une politique de sécurité pour les usagers du système ainsi qu'une politique de sécurité pour les techniciens responsables de l'installation des serveurs. Vos politiques et mécanismes doivent satisfaire toutes les volontés du SST.

1. Quelles menaces voyez-vous à la sécurité du système que le SST veut mettre en place. Utilisez la classification STRIDE et n'oubliez pas de spécifier les effets des menaces identifiées.
2. Donnez les grandes lignes d'une politique de sécurité pour les usagers du système de stockage et partage de document du SST. Les usagers sont d'une part, les agents en déplacement et, d'autre part, les employés ayant accès aux documents. Ne donnez que les objectifs, les dispositions générales et dispositions aux usagers. Pour chaque disposition, indiquez les menaces qu'elle vise à éviter.
3. Donnez les grandes lignes d'une politique de sécurité pour les techniciens responsables de l'installation ou la mise à niveau des serveurs du système. Ne donnez que les objectifs, les dispositions générales et dispositions aux techniciens. Pour chaque disposition, indiquez les menaces qu'elle vise à éviter.
4. Mentionnez les mécanismes que vous utiliseriez pour la réalisation de votre politique. Ces mécanismes n'ont pas tous à être de nature électronique. Ils devraient permettre d'atteindre les objectifs de votre politique contre les menaces que vous avez identifiées. Pour chacun des mécanismes, indiquez les dispositions de vos politiques qui peuvent être réalisées en utilisant celui-ci.

**********FIN**********