IFT6271–Sécurité Informatique
(Plan de cours –hiver 2014)

Louis Salvail[1]

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

1 Quand et où

Le cours aura lieu au rythme de deux périodes de 90 minutes par semaine. La plupart du temps, environ une heure par semaine sera consacrée à la résolution d'exercices.

Mardi 17:30-19:30 $\Rightarrow$ local 1411, Pav. André-Aisenstadt.
Jeudi 17:30-19:30 $\Rightarrow$ local Z-215, Pav. McNicoll.

Le premier cours aura lieu le mardi 7 janvier 2014.

2 Matériel et Prérequis

Il n'y a pas de livre pour ce cours. Des notes de cours sous forme électroniques seront mises à disposition à mesure que le trimestre progresse. Quelques lectures additionnelles accompagneront le cours. Le site du cours est le suivant:

`www.iro.umontreal.ca/~salvail/securite/index.html` .

Ce cours s'adresse à des étudiants aux compétences diverses. Sans être un prérequis, il serait préférable que l'étudiant ait quelques connaissances préalables en informatique. Les mathématiques qui sous-tendent bien des mécanismes de sécurité seront réduites à leur plus simple expression. Cependant, elles ne peuvent être complètement évacuées du sujet et l'étudiant devra montrer un minimum d'ouverture sur ce plan.

Ce cours traite de la sécurité informatique d'un point de vue descriptif et théorique. Le but du cours est d'introduire l'étudiant aux mécanismes de sécurité ainsi qu'aux faiblesses communes des systèmes informatiques. Les travaux pratiques ne demanderont pas de connaissances approfondies en informatique. Un seul devoir vous demandera d'utiliser votre ordinateur pour autres choses que sa rédaction.

3 Plan

Le cours traitera des sujets suivants dans l'ordre approximatif indiqué ci-dessous:

1. Introduction
2. Un peu de maths
3. Cryptographie à clé secrète:

   - Chiffrement symétrique
   - Intégrité de l'information
4. Cryptographie à clés publiques
   - Chiffrement asymétrique
   - Signatures numériques
   - Infrastructures à clés publiques
5. Authentification et identification
6. Sûreté des réseaux
7. Mécanismes de sécurité des systèmes
8. Quelques écueils courants
9. Politiques de sécurité et contrôles d'accès
10. Systèmes de paiements électroniques (à confirmer)

4 Évaluation

L'évaluation du cours se fera en deux parties:

1. Trois devoirs, possiblement par équipes de deux. (40%)
2. Un examen final. (60%)