Direction de l'Enseignement de **S**ervice en **I**nformatique
Université de Montréal

Abdeltouab Belbekkouche
belbekka@iro.umontreal.ca

IFT2830 : Sécurité des systèmes informatiques

Hiver 2016

Plan de cours

Objectifs

Nul ne peut aujourd'hui ignorer les dangers liés à l'utilisation d'Internet : virus, spam et pirates informatiques sont les maîtres mots utilisés par les médias. À domicile comme au bureau il devient indispensable de connaître les risques liés à l'utilisation d'Internet et les principales parades.

Ce cours a pour but d'initier l'étudiant aux notions de base de la sécurité des systèmes informatiques. Plus précisément, il permet à l'étudiant de se familiariser avec quelques composantes fondamentales de la sécurité informatique, à savoir :

- Les menaces informatiques;
- Les malwares;
- Les techniques d'attaque;
- La cryptographie et les protocoles sécurisés;
- Les dispositifs de protection;
- La sécurité des réseaux sans fil;
- La sécurité des ordinateurs portables, smartphones et tablettes;
- La sécurité des applications Web;
- La sécurité et le système d'information.

Préalables

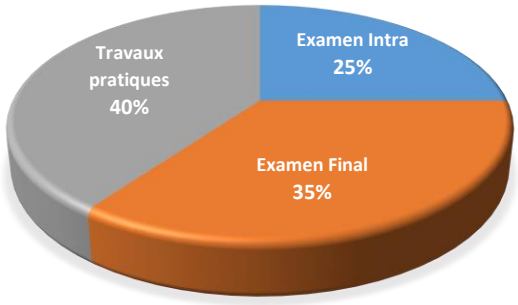
Le cours IFT1810 (Initiation à la programmation (C et Java)). Il est également recommandé à l'étudiant d'avoir un minimum d'expérience et d'autonomie avec les systèmes d'exploitation Windows et/ou Linux.

Déroulement du cours

Exposés magistraux avec des démonstrations pratiques selon la pertinence. Le cours se veut interactif, ainsi, la participation des étudiants est fortement encouragée. Le matériel du cours sera mis à jour au fur et à mesure sur la page du cours dans **Studium**.

Évaluation

- Examen intra*: 25 %
- Examen final*: 35 %
- Travaux pratiques : 40 %



**Un seuil de 40 % sur l'ensemble pondéré des deux examens est requis pour réussir le cours*

Abdeltouab Belbekkouche
belbekka@iro.umontreal.ca

Travaux pratiques

Il y aura quatre (4) travaux pratiques à remettre pour ce cours. Les énoncés des travaux pratiques seront rendus disponibles au fur et à mesure sur la page du cours dans **Studium**. Les remises se feront également via la page du cours dans **Studium**.

Horaire du cours

Cours théoriques

Jour	Heure	Date	Local
Mardi	18h30 - 20h29	05/01/2016 - 16/02/2016	Z-305 Pav. Claire-McNicoll
Mardi	18h30 - 20h29	08/03/2016 - 12/04/2016	Z-305 Pav. Claire-McNicoll

Démonstrations

Jour	Heure	Date	Pavillon, local
Mardi	20h30 – 22h29	12/01/2016 - 23/02/2016	S-118 Pav. Roger-Gaudry
Mardi	20h30 – 22h29	08/03/2016 - 12/04/2016	S-118 Pav. Roger-Gaudry

Démonstrateur : Ayman Khlif (khlifaym@iro.umontreal.ca)

Examens*

Examen	Jour	Heure	Date	Local
Intra	Mardi	18h30 - 20h29	23/02/2016	Z-240 Pav. Claire-McNicoll
Final	Mardi	18h30 - 21h29	19/04/2016	Z-240 Pav. Claire-McNicoll

* À revérifier avant l'examen

Note

Le plagiat à l'Université de Montréal est sanctionné par le règlement disciplinaire sur la fraude et le plagiat concernant les étudiants. Pour plus de renseignements, consultez l'URL http://www.integrite.umontreal.ca

Abdeltouab Belbekkouche
belbekka@iro.umontreal.ca

Contenu du cours

Thème	Contenu
1) Introduction à la sécurité informatique	• Objectifs de sécurité et fonctions associés • Domaines d'application de la sécurité • Architecture de sécurité
2) La sécurité et le système d'information	• Politiques de sécurité • Analyse des risques
3) Les malwares	• Virus • Vers réseau • Chevaux de Troie • Bombes logiques • Spywares (espiogiciels) • Keyloggers • Spam (Pourriel) • Rootkits
4) Les menaces informatiques	• Méthodologie d'une attaque réseau • Intrusion • Nettoyage des traces Réalité des menaces
5) Les techniques d'attaque	• Attaques de mots de passe • Usurpation d'adresse IP • Attaques par déni de service • Attaques « man in the middle » • Attaques par débordement de tampon • Attaque par ingénierie sociale
6) Cryptographie et protocoles sécurisés	• Chiffrement symétrique et asymétrique • Certificats et signature électronique • Protocoles SSL, SSH, Secure HTTP
7) Dispositifs de protection	• Antivirus • Pare-feu (Firewall) • Serveurs mandataires (proxy) • Systèmes de détection d'intrusion (IDS) • Réseaux privés virtuels (VPN)
8) Sécurité des réseaux sans fil	• « War driving » • Risques en matière de sécurité • Sécurisation d'un réseau sans fil
9) Sécurité des ordinateurs portables, smartphones et tablettes	• La protection matérielle • La protection des données • La protection des smartphones et des tablettes
10) Sécurité des applications Web	• Vulnérabilité des applications Web • Falsification des données • Manipulation des d'URL • Attaque par injection de commandes SQL

Abdeltouab Belbekkouche
belbekka@iro.umontreal.ca

Références

Aucun livre n'est exigé pour ce cours. Les références suivantes peuvent s'avérer utiles :

- S. Ghernaouti, *Sécurité informatique et réseaux*, 4ème édition, Dunod, 2013.
- J-F. Pillou, J-P. Bay, *Tout sur la Sécurité informatique*, 3ème édition, Dunod, 2013.
- M. T. Simpson, K. Backman, J. E. Corley, *Hands-On Ethical Hacking and Network Defense*, Course Technology, 2012.
- Mark Ciampa, Security+ Guide to Network Security Fundamentals. 4th edition. 2011.
- R. Panko, *Sécurité des systèmes d'information et des réseaux*, Pearson Education, 2004.
- D. Salomon, *Foundations of Computer Security*, Springer, 2006.
- H. F. Tipton, M. Krause, *Information security management handbook*, 5th edition, Auerbach, 2004.
- M. Bishop, *Computer security: Art and science*. Addison-Wesley, 2002.
- E. Skoudis, *Counter hack: A step-by-step Guide to Computer Attacks and Effective Defenses*, Prentice Hall, 2002.
- W. Stallings, *Network security essentials*, 2nd edition, Prentice-Hall, 2003.
- D. R. Stinson, *Cryptography: Theory and practice*. 2nd edition, CRC Press, 2002.