UNIVERSITÉ DE SHERBROOKE

Département d'informatique
IFT606 – Sécurité et cryptographie
Plan de cours
Hiver 2016

Enseignants

Mohammed Ouenzar et Marc Verreault

Courriel:	Mohammed.Ouenzar@usherbrooke.ca, maverreault@gmail.com
Local:	D6-0047
Téléphone:	(819) 821-8000 postes 21566 et 15069
Disponibilité :	Sur rendez-vous

Enseignant responsable : Mohammed Ouenzar

Horaire

Exposé magistral :	Lundi	15 h 30 à 17 h 20	salle D3-2037
	Mercredi	13 h 30 à 15 h 20	salle D3-2037

Description officielle de l'activité pédagogique[1]

Objectifs	Être capable d'évaluer et de gérer les risques et la sécurité d'un système informatique. Être capable de définir une politique de sécurité. Savoir comment assurer la confidentialité et l'intégrité des données. Connaître les divers types d'attaques et leurs parades.
Contenu	Concepts de base de la sécurité informatique. Confidentialité. Authentification. Intégrité. Contrôle des accès. Cryptographie. Signature électronique. Certificats. Gestion de clés. Attaques et parades. Virus. Architectures. Coupe-feu. Réseaux virtuels privés. Politiques de sécurité. Méthodologies, normes et analyse de risques.
Crédits	3
Organisation	3 heures d'exposé magistral par semaine 6 heures de travail personnel par semaine
Préalable	MAT115
Concomitante	IFT585

[1] http://www.usherbrooke.ca/fiches-cours/ift606

1 Présentation

1.1 Mise en contexte

L'informatisation est une tendance dans tous les domaines. Les non-informaticiens ne réalisent pas à quel point les risques de sécurité sont différents. L'accès et les échanges des données confidentielles sont rapides, faciles et invisibles en comparaison aux anciennes méthodes : le contexte a changé.

La sécurité informatique se définit comme suit : c'est l'état dans lequel l'information est hors de danger. En tant qu'analyste informatique, vous aurez à assurer la sécurité de l'information contenue dans les systèmes dont vous aurez la responsabilité.
Le cours de sécurité et cryptographie vous permettra de comprendre les menaces informatiques, les moyens pour les contrer, pour les prévenir et pour réagir le cas échéant. De plus, vous verrez de manière plus globale, comment favoriser et définir des environnements plus sécuritaires.

Des exemples concrets actuels ainsi que des exercices pratiques seront utilisés pour consolider vos connaissances.
Un projet de cours, basé sur vos intérêts, vous permettra de mettre en pratique vos connaissances acquises tout en exerçant vos aptitudes à les communiquer.

1.2 Objectifs spécifiques

À la fin de cette activité pédagogique, l'étudiante ou l'étudiant sera en mesure de :

1. connaître les principaux enjeux de la sécurité;
2. comprendre les mécanismes de cryptographie et leur utilité;
3. savoir les mettre en pratique selon le contexte;
4. connaître les types d'attaques informatiques et leurs impacts;
5. connaître les moyens de défense contre ces attaques;
6. identifier les vulnérabilités des architectures et les solutions;
7. connaître le processus d'enquête informatique;
8. prendre conscience d'enjeux spécifiques de l'industrie.

1.3 Contenu détaillé

Thème	Contenu	Heure	Objectifs	Travaux	Responsables
1	Introduction - Contexte - Objectifs et évaluation	1	1		M. Verreault M. Ouenzar
2	Cryptographie - Historique - Encryption symétrique - Encryption asymétrique - Fonctions de hachage - Cryptographie appliquée - Exercices dirigés (2h)	6	2,3		M. Ouenzar
3	Attaque - Contexte - Vulnérabilités - Types d'attaques - Outils - Le processus - Applications pratiques (laboratoire)	7	4	Devoir : *Crypto-attaque*	M. Verreault et M. Ouenzar
4	Défense - Défense vs les types d'attaques - Défense vs l'architecture - Défense organisationnelle et facteur humain - Meilleures pratiques	6	5,6		M. Verreault
5	Architecture de sécurité - Définition et principes - Standards - Exemples pratiques	4	6		M. Verreault
6	Enquête informatique	2	7		M. Verreault et M. Ouenzar
7	Projet de cours - Accompagnement de projet - Présentation orale	14		Rapport et présentation	M. Ouenzar

40

2 Organisation

2.1 Calendrier

Date	Jour	Durée	Thèmes
2016-01-06	Mercredi	2	Introduction et Cryptographie
2016-01-11	Lundi	2	Cryptographie
2016-01-13	Mercredi	2	Cryptographie
2016-01-18	Lundi	2	Cryptographie
2016-01-20	Mercredi	2	Cryptographie
2016-01-25	Lundi	2	Attaque; *Dernier jour de modification des activités pédagogiques*
2016-01-27	Mercredi		*Congé universitaire*
2016-02-03	Lundi	2	Attaque; Devoir *: Crypto-attaque énoncé*
2016-02-08	Mercredi	2	Défense; *Projet : Sujets proposés*
2016-02-10	Lundi	2	Défense
2016-02-15	Mercredi	2	Défense;
2016-02-17	Lundi	2	Architecture de sécurité
2016-02-22	Mercredi	2	Architecture de sécurité;
2016-02-24	Lundi		*Levée des cours, examens périodiques*
2016-02-29	Mercredi		*Levée des cours, examens périodiques*
2016-03-02	Lundi		*Relâche des activités pédagogiques*
2016-03-07	Mercredi		*Relâche des activités pédagogiques*
2016-03-09	Lundi	2	Accompagnement de projet; ***Remise devoir***
2016-03-14	Mercredi	2	Accompagnement de projet
2016-03-16	Lundi	2	Accompagnement de projet
2016-03-21	Mercredi	2	Accompagnement de projet
2016-03-23	Lundi	2	Accompagnement de projet
2016-03-28	Mercredi	2	Conférencier (Possiblement à une autre période, selon disponibilité)
2016-03-30	Lundi		*Lundi Pâques*
2016-04-04	Mercredi	2	***Présentation** orale projet **; Remise** rapport final projet*
2016-04-06	Lundi	2	***Présentations** orales projet*
2016-04-11	Mercredi	2	***Présentations** orales projet*
2016-04-13	Lundi	2	*Dernier jour de cours et de travaux pratiques*
2016-04-18	Mercredi		*Examens finaux*
2016-01-06	Lundi		*Examens finaux*
	TOTAL	44	

2.2 Évaluation

no	Élément	Valeur
1	Devoir	15%
2	Projet	25%
3	Examen périodique	25%
4	Examen final	35%

Conformément à l'article 17 du Règlement facultaire d'évaluation des apprentissages[2], l'enseignant peut retourner à l'étudiante ou à l'étudiant tout travail non conforme aux exigences quant à la qualité de la langue et aux normes de présentation.
Le plagiat consiste à utiliser des résultats obtenus par d'autres personnes afin de les faire passer pour sien et dans le dessein de tromper l'enseignant. Si une preuve de plagiat est attestée, elle sera traitée en conformité, entre autres, avec l'article 8.1.2 du Règlement des études[3] de l'Université de Sherbrooke. L'étudiant ou l'étudiante peut s'exposer à de graves sanctions dont automatiquement un zéro (0) au devoir ou à l'examen en question.
Ceci n'indique pas que vous n'ayez pas le droit de coopérer entre deux équipes tant que la rédaction finale des documents et la création du programme reste le fait de votre équipe. En cas de doute de plagiat, l'enseignant peut demander à l'équipe d'expliquer les notions ou le fonctionnement du code qu'il considère comme étant plagié. En cas de doute, ne pas hésiter à demander conseil et assistance à l'enseignant afin d'éviter toute situation délicate par la suite.

2.3 Échéancier des travaux

Travail	Thème	Énoncé ou choix projet	Date de remise
Devoir	Crypto-attaque	2016-02-03	2016-03-09
Projet	Projet pratique avec notions de sécurité informatique	2016-02-22	À partir du 2016-04-04 : présentations orale 2016-04-13 Date limite remise rapport final

2.4 Devoir et projet

Le devoir pourront être réalisés en équipe de deux personnes au maximum. Le projet devra être réalisé en équipe de trois à cinq personnes. Le projet sera évalué lorsqu'il sera remis. Il peut y avoir une présentation de projet, dépendant des critères qui seront définis au cours de la session.

2.5 Directives particulières

Il est strictement interdit de poser tout acte pouvant nuire au bon fonctionnement des équipements et des ressources informatiques et de télécommunication ou du réseau, entre autres, par l'insertion et la propagation d'agents malicieux informatiques ou par la saturation de ressources.

2.6 Outil de travail

- Kali Linux (Backtrack)[4]

[2] http://www.usherbrooke.ca/accueil/fileadmin/sites/accueil/documents/direction/politiques/2500-008-sciences.pdf
[3] http://www.usherbrooke.ca/programmes/etude
[4] http://www.kali.org/downloads/

3 Références

Les livres suivants, en format électronique en-ligne de la Bibliothèque Nationale du Québec, sont disponibles sans frais pour tout citoyen résident au Québec. Notez que cette liste n'est pas nécessairement à jour et que vous devez consulter l'outil MOODLE, dans lequel vous retrouverez un tableau sommaire d'étude avec l'ensemble de la documentation liée.

3.1 Cryptographie

[ASSELIN] Éric Asselin, Gabriel Girard: *Notes de cours - Cryptographie* juin 2012 «*Cryptographie notes de cours Gabriel Girard et Éric Asselin.pdf*».

3.2 Attaque

[CONVERY] Sean CONVERY : *Network Security Architectures,* Cisco Press, 2004.
[COLE] Eric COLE: *Hackers Beware*, Sams, 2001.
[GREGG] Michael Gregg: *Certified Ethical Hacker (CEH) Cert Guide,* 2013.
[KENNEDY] David Kennedy; Jim O'Gorman; Devon Kearns; Mati Aharoni, *Metasploit*, No Starch Press, 2011.
[AGARWAL] Monika Agarwal; Abhinav Singh, *Metasploit Penetration Testing Cookbook - Second Edition*, Packt Publishing, 2013.
[PRITCHETT] Willie L. Pritchett; David De Smet, *Kali Linux Cookbook*, Packt Publishing, 2013

3.3 Défense

[SCAMBRAY] Scambray Joel; Liu Vincent; Sima Caleb, *Hacking exposed: WEB Applications*, McGraw-Hill, 2010.
[MCCLURE] Stuart McClure; Joel Scambray; George Kurtz, *Hacking Exposed ™ 7: Network Security Secrets & Solutions*, McGraw-Hill, 2012.
[CACHE] Johnny Cache; Joshua Wright; Vincent Liu, *Hacking Exposed™ Wireless: Wireless Security Secrets & Solutions, Second Edition*, McGraw-Hill, 2010.
[SP800-53A] Patrick D. Gallagher, *Building Effective Security Assessment Plans*, National Institute of Standards and Technology, 2010.
[SP800-53r4] NIST Special Publication, *Security and Privacy Controls for Federal Information Systems and Organizations*, NIST, 2013.
[CHAPLIN] Mark Chaplin, Jason Creasey, *The 2011 Standard of Good Practice for Information Security*, 2011.
[SANS] SANS Institute, *Top 20 Critical Security Controls*, 2013.
[MANICO] Jim Manico/owasp.org , *XSS (Cross Site Scripting) Prevention Cheat Sheet,* 2014.

3.4 Enquêtes

[COWEN] David Cowen, *Computer Forensics InfoSec Pro Guide*, McGraw-Hill, 2013.