UNIVERSITÉ DE SHERBROOKE
Département d'informatique

IFT 606
Sécurité et cryptographie

Plan de cours
Hiver 2012

Enseignant : Jean-Philippe Luiggi
Courriel : jean-philippe.luiggi@usherbrooke.ca
Local : D6-0047
Téléphone : (819) 821-8000 (poste 63061)
Site : à venir
Disponibilité : sur rendez-vous

Horaire :

Lundi	16h30 à 17h20	salle D3-2039
Mercredi	15h30 à 17h20	salle D3-2039

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'omniprésence de l'informatique dans tous les aspects de la vie courante a comme corollaire d'apporter un nombre toujours croissant de nuisances. Ces nuisances n'affectent pas seulement les informaticiens mais aussi les personnes appelées “Monsieur ou Madame Tout le monde”. La simple ménagère qui souhaite faire ses comptes sur Internet s'expose à bien des tracas si elle ne prend pas un minimum de précautions une fois le PC familial laissé libre après la séance quotidienne de promenade sur le Net par les enfants.

Et ce qui est vrai pour les personnes l'est encore plus pour les sociétés, s'il fallait citer quelques-uns des risques encourus, nous aurions le choix entre vol de données personnelles, espionnage et cessation d'activités, que ce soit par la destruction des moyens informatiques ou le manque de procédures afin de traiter une problématique de sécurité précise.

Les notions afférentes à la sécurité informatique ne sont pas à prendre à la légère, elles ne sont plus uniquement une affaire de spécialistes et se doivent d'être prises en compte par tout un chacun, que ce soit dans les sociétés avec des procédures de fonctionnement strictes ou par les particuliers avec une sensibilisation à une bonne “hygiène d'utilisation” et une éducation à l'utilisation de l'outil informatique.

1.2 Objectifs spécifiques

À la fin de cette activité pédagogique, l’étudiante ou l’étudiant sera capable :

1. de comprendre les notions afférentes à la sécurité informatique ;
2. de savoir évaluer celle-ci dans un cadre précis ;
3. de préparer ses défenses ;
4. de comprendre les différents types d’attaques ;
5. de gérer les incidents de sécurité ;
6. de mettre en œuvre une méthodologie de traitement de la sécurité informatique ;
7. de connaître les normes en sécurité informatique ;
8. de conduire une analyse de risques.

1.3 Contenu détaillé

Thème	Contenu	Heures	Objectifs	Travaux
1	Présentation des notions de sécurité informatique - Définition de la sécurité informatique - Objectifs de la sécurité - Ce qu'il faut et ne pas faire - Principes de base	3	1	
2	Exemple de cas concrets de problèmes de sécurité - Morris Worm - Attaques sur l'Arpanet - Duel Mitnick/Shimomura -Attaques sur l'infrastructure de l'Internet	1	1, 5	
3	La guerre (informatique) - Rappels historiques - De nos jours	2	1	
4	Introduction et applications de la cryptographie - Historique - Fonctions de hachage - Les clés symétriques - Les clés asymétriques - Exemples de système cryptographiques (DES, AES, RSA) - Certificats et signatures numériques - Infrastructures à clé publique : PKI - Utilisation dans la vie de tous les jours : SSL/TLS, SSH, VPN	6	3	A
5	L'art de la cryptanalyse : méthodes pour déchiffrer des messages	2	3	
6	Concepts mathématiques liés à la cryptographie	6	3	
7	Réseautique et architecture - Rappels de base sur les réseaux - Les différents protocoles réseaux - Comprendre TCP/IP, détecter les anomalies	2	2	
8	Les différents phases préalables aux attaques - Obtenir de l'information - Divers types de reconnaissances	3	4	
9	Penser la défense - Préparer le système d'informations aux agressions - Savoir bâtir une architecture globale	2	3	
10	Les différents types d’attaques - Les couches réseaux - Les couches applicatives	4	4	A
11	Les moyens de défense - Rechercher les outils en notre possession - Savoir les placer - En développer	3	3	A
12	Méthodes d’analyse en sécurité - Avoir une vue sur l'état de l'art - Vérifier ce qu'elles proposent	2	6	A
13	Normes, lois - Normes ISO 17999, ISO 27001 - Cadre législatif	2	7, 8	
14	Certifications - SANS - CISSP - CISM	1	7	
15	Conclusion+rappels	1		

La lettres "A" correspond à l’analyse/conception.

2 Organisation

2.1 Méthode pédagogique

Une semaine comprend trois heures de présence en classe : dont trois heures de cours dit théorique. Tous les thèmes du cours seront abordés de la même manière : présentation du contenu, mise en relation (si possible) avec des exemples réels.

2.2 Calendrier du cours

	Semaine du		Thème
1	09-01-2012		1 (3h)
2	16-01-2012		2 (1h) – 3 (2h)
3	23-01-2012	Activités étudiantes – ME 25 janvier	7 (1h)
4	30-01-2012*		7 (1h) – 9 (2h) – 11 (1h)
5	06-02-2012*		11 (2h) – 8 (2h)
6	13-02-2012*		8 (1h) – 10 (3h)
7	Période du 18 au 24 février	Examen intra	
8	27-02-2012		10 (1h) – 6 (2h)
9	05-03-2012	Relâche	
10	12-03-2012*		6 (4h)
11	19-03-2012*		4 (4h)
12	26-03-2012		4 (2h) – 5 (1h)
13	02-04-2012		5 (1h) – 12 (2h)
14	09-04-2012	Congé universitaire LU 9 avril	13 (2h)
15	16-04-2012*		14 (1h) – 15 (1h)
16	Période du 17 au 27 avril	Examen final	

* Des séances spéciales auront lieu les lundis 15h30 à 16h20 pour les dates suivantes : 30 janvier, 6 février, 13 février, 12 mars, 19 mars et 16 avril (D3-2039).

2.3 Évaluation

Devoirs (5 x 6 %) : 30 %
Examen périodique: 30 %
Examen final: 40 %

2.4 Échéancier des travaux

TP	Thème	Remise de l'énoncé	Date de remise
1	Recherche et analyse de données	20-01-2012	03-02-2012
2	Architecture réseau	03-02-2012	24-02-2012
3	Attaquer une cible	24-02-2012	16-03-2012
4	Cryptographie	16-03-2012	30-03-2012
5	Cryptographie II	30-03-2012	13-04-2012

3 Documentation

Michael Goodrich,Roberto Tamassia : ”Introduction to Computer Security ”
ISBN : 0-3215-1294-4

Raymond Panko : “Sécurité des systèmes d’information et des réseaux”
ISBN : 2-7440-7054-8

Susan Young and Dave Aitel : “The Hacker’s Handbook”
ISBN : 0-8493-0888-7