INF4471
Introduction à la sécurité informatique

Plan de cours

Responsable(s) du cours

Coordination : KILLIJIAN, Marc-Olivier
PK-4740
killijian.marc-olivier.2@uqam.ca
https://kirija.github.io

Enseignement :

KILLIJIAN, Marc-Olivier
PK-4740
killijian.marc-olivier.2@uqam.ca
https://kirija.github.io
Groupes : 020

Description du cours

Il s'agit d'un cours d'hygiène informatique et d'introduction à la sécurité informatique. Les objectifs sont donc souvent duals entre application et théorie. Au fil des séances, nous verrons notamment les points suivants.

Principes et concepts fondamentaux de la sécurité des systèmes informatiques. Principaux objectifs de sécurité : confidentialité, intégrité, disponibilité, authentification, non-répudiation, contrôle d'accès. Typologie des attaques et menaces : fuites, modifications, dénis de service.

Introduction aux mécanismes de sécurité modernes : systèmes de chiffrement symétriques et asymétriques ; codes d'authentification de messages et signatures électroniques ; fonctions de hachage ; protocoles sécuritaires : authentification, contrôle d'accès.

Sécurité des réseaux : gestion et infrastructure de clés ; étude de la sécurité de protocoles existants (TLS, IPSec) ; protocoles d'authentification dans les réseaux sans fil (WEP, WPA et WPA2) ; surveillance et détection d'intrusion ; appareils mobiles.

Sujets avancés : introduction à la protection de la vie privée ; sécurité en infonuagique ; sécurité de l'internet des objets ; Bitcoin et blockchain.

Gestion des incidents de sécurité et améliorations des systèmes : mécanismes de recouvrement. Analyse de risque. Gestion des vulnérabilités techniques. Éducation des usagers. Considérations légales, politiques et éthiques. Politiques et modèles de sécurité.

Objectif du cours

Introduire les étudiants à l'hygiène informatique et aux différents aspects de la sécurité des systèmes informatiques. Sensibiliser les étudiants aux risques et menaces. Présenter les techniques permettant d'assurer la sécurité des systèmes d'information. Décrire les méthodes de mitigation du risque.

À la fin de ce cours, l'étudiant devra être en mesure de :

- comprendre l'ensemble des problématiques de la sécurité informatique et distinguer les principaux objectifs de sécurité ;
- manipuler de façon sécuritaire les outils informatique ;
- expliquer le fonctionnement et justifier l'utilisation des principaux mécanismes de sécurité : chiffrement, signature, hachage, protocoles, etc. ;
- identifier les risques et les menaces, actuels et futurs, auxquels fait face un système ;
- proposer des mesures de contrôle appropriées.

Contenu du cours

Introduction. Problématique de la sécurité : confidentialité, authentification, intégrité, traçabilité, disponibilité, non-répudiation, respect de la vie privé, contrôle d'accès. Vulnérabilités, menaces à la sécurité et attaques. Techniques de base en sécurité : Terminologie. Notion de confiance. Analyse de risque. Principes et politiques de sécurité. Éducation des usagers, hygiène informatique personnelle et professionnelle. Droits et organisation de la sécurité informatique.

Canaux cachés. Fuites d'information matérielles, métadonnées, réseau. Respect de la vie privée et lien avec la sécurité informatique. Outil de traçage, traces numériques. Attaques par inférence et méthodes d'assainissement. Protection des données par k-anonymat et confidentialité différentielle. Technologies de protection de la vie privée (réseaux de communication anonyme, accréditations anonymes, retrait privé d'information).

Enjeux géopolitiques, économiques et étatiques de la sécurité informatique. Agences nationales de sécurité, espionnage. Méthodes d'appréciation et d'analyse de risques : évaluation, analyse, acceptation, assurance. Vie privée et technologies de géolocalisation : enjeux, attaques et défenses.

La fraude sur Internet. Les différents types d'attaques et les risques et menaces associées : hameçonnage, dénis de service, vol d'identité, botnets, rançongiciels. Economie de la sécurité et de l'insécurité, marché des failles de sécurité.

Cryptographie symétrique (clé privée). Arithmétique modulaire. Principes de Kerckhoffs. Exemples de chiffrements historiques et de mécanismes de base : transposition, permutation. Caractérisation des systèmes de chiffrement. Cryptanalyse et attaques. Notions de base fondamentales : entropie, redondance. Chiffrement à sécurité inconditionnelle : masque jetable. Systèmes de chiffrement symétriques modernes (DES, AES). Modes de fonctionnement : ECB, CBC, CTR. Chiffrement par flux (RC4).

Communications anonymes. Systèmes d'échanges pair-à-pair. Darkweb, le routage en oignon et TOR. La chaine de bloc et les monnaies cryptographiques. Les messageries sécurisées. VPNs. Accréditations anonymes.

Malware et antivirus. Aspects historiques. Typologie des malware et la métaphore anthropomorphe (virus, ver, troyen et bombes logiques). Contremesures, analyse de malware, pots-de-miel, systèmes de détection d'intrusion, antivirus, patches.

Cryptographie asymétrique (clé publique). Historique et propriétés. Bases mathématiques : calcul entier, PGCD, modules et exponentiation modulaire. RSA. Fonctions à sens unique. Intégrité des données et authentification de messages. Génération pseudo-aléatoire. Introduction au chiffrement homomorphe.

Courriel, pourriel, authentification, signatures électroniques et infrastructure de gestion de clé. Problématique et enjeux économiques des pourriels et de leur détection. Signature numérique DSA et RSA. Le logarithme discret. Gestion et infrastructure de clés (Diffie-Hellman, attaques de l'homme du milieu). Infrastructure publique, certificats, chaines de certificats, X.509, PGP.

Mots de passe et authentification de messages. Fonctions de hachage (MD5, SHA-1, SHA-3). Codes d'authentification de message (HMAC, CBC-MAC). Introduction aux protocoles d'authentification. Les mots-de-passe et leur propriétés. Gestionnaires de mots-de-passe. Attaques et outils d'évaluation de la robustesse des mots de passe. Authentification biométrique.

Disques dur chiffrés et forensique. Comment et pourquoi chiffrer un disque dur. La forensique, les enjeux et techniques. L'expertise judiciaire, la réponse à incident de sécurité.

Sécurité des systèmes répartis et de réseaux. Rappel réseau (TCP/IP, équipement). Menaces spécifiques : écoute illicite, imposture, déni de service, brouillage. Caractéristiques des médiums de transmission. Capture de paquets, pare-feus, proxies, détection d'intrusion. Réseaux privés virtuels. Les protocoles IPSec, SSH et SSL et certaines attaques. Authentification dans les réseaux Wi-Fi (WEP, WPAs) et le protocole Bluetooth.

Formule pédagogique

Chaque séance sera composée de différentes activités, chacune obligatoire et susceptible d'être évaluée dans un devoir ou un examen :

- Séance de cours (3h)
- Laboratoire (2h)
- Lectures
- Ecoute de ballados, vidéos

Des activités optionnelles seront parfois proposées, possiblement en langue anglaise.

Calendrier

#Semaine	Cours
1	Introduction
2	Fuite d'information
3	Geolocalisation - Intelligence économique
4	Fraude sur Internet
5	Cryptographie symmétrique
6	Communications anonymes
7	**Présentations**
8	Maliciels et antivirus
9	Cryptographie asymmétrique
10	Courriels et pourriels
11	Mots de passe
12	Chiffrement de disque dur
13	Sécurité réseau 1
14	Sécurité réseau 2
15	**Examen final**

Modalités d'évaluation

- Présentation d'un sujet lié à la sécurité (en équipe et co-évaluées le 19 octobre) : 20%
- Devoir 1 (à rendre le 10 octobre à 23h55) : 25%
- Devoir 2 (à rendre le 14 novembre à 23h55) : 25%
- Examen final (14 décembre) : 30%

Présentations (20%) - 19 octobre

A réaliser par équipe de 5 étudiants, une présentation d'une durée de 8 à 10 minutes autour des problématiques de sécurité sur un sujet spécifique à prendre dans la liste suivante, ou à proposer et à faire valider par le Professeur. Ces capsules seront ensuite accessibles à tous les étudiants, qui participeront à leur évaluation. Il s'agit de présenter les problèmes de sécurité soulevés, ou traités, par le sujet en question, l'évaluation porte sur l'objectif #1 du cours : "comprendre l'ensemble des problématiques de la sécurité informatique et distinguer les principaux objectifs de sécurité".

Chaque équipe devra sélectionner un sujet distinct.

Sujets potentiels : les fuites de données ; le paiement sans contact ; le passeport vaccinal (CoVid) ; les outils de visio-conférence (Zoom, etc.) ; les bug bounty ; red-team vs. blue-team ; le tatouage de vidéo ; la cryptographie quantique ; la cryptographie post-quantique ; le chiffrement homomorphe ; e-démocratie ; vote électronique et machines à voter ; authentification biométrique ; sécurité offensive ; évaluation des risques de sécurité ; etc.

Devoirs (50 %) - 10 octobre et 14 novembre

A deux occasions au cours de la session, des devoirs écrits notés permettront aux étudiants d'approfondir les sujets vus en cours ou encore de mettre en pratique et de vérifier expérimentalement certains des concepts présentés en classe. Les devoirs toucheront à différents sujets en sécurité informatique. L'écriture de programmes courts sera potentiellement nécessaire pour la réalisation des devoirs.

Examen final (30 %) - 14 décembre

Examen à livre ouvert, portant sur l'ensemble de cours.

Prenez note que la correction des exercices et examens tient abondamment compte des explications fournies. Il est donc avantageux d'exposer votre travail de façon claire et dans un langage correct. Une réponse correcte obtenue au terme d'un raisonnement invalide ou flou ne vaut pas grand chose. Par contre, un raisonnement valide, conduisant à une réponse erronée à cause d'erreurs mineures vaut beaucoup plus. Dans le doute, il vaut mieux être explicite que succinct.

Notes

Les règlements de l'UQAM concernant le plagiat seront strictement appliqués. Pour plus de renseignements, consultez le site suivant : http://r18.uqam.ca

Tout travail que vous soumettez doit être le fait de votre propre travail. Vous pouvez échanger avec vos collègues sur les travaux, les approches de solutions, mais les idées et solutions que vous soumettez doivent émaner de votre propre réflexion. Dans le cas de programmes, vous devez créer et coder votre propre code source, et le documenter vous même. Une fois le programme écrit, il est possible de se faire aider pour le déboguage.

En cas de doute sur l'originalité des travaux, un test oral pourra être exigé.

Une pénalité de retard de 10% par jour ouvrable sera appliquée sur les travaux remis après les dates prévues. Il est de la responsabilité de l'étudiant de se faire des copies de ses travaux.

Matériel et logiciels utilisés

Le cours se donne en présentiel, mais afin d'être capable de passer en mode distanciel s'il le fallait, il vous faut un ordinateur connecté à Internet, capable de lire des vidéos et d'écouter des ballados. Il vous faudra également installer le logiciel Zoom. Certains laboratoires vous demanderont d'installer le logiciel Oracle VirtualBox https ://www.virtualbox.org/wiki/Downloads et de lancer une machine virtuelle Linux d'une taille de plusieurs dizaines de Go. Afin de ne pas avoir de problème, il vous est donc recommandé d'avoir au minimum 100 Go d'espace disque libre. Tout système (Windows, Linux, Macintosh, Solaris) convient a priori. Il sera nécessaire de disposer d'une clé USB **vierge** d'au moins 8 Go.

Médiagraphie

Sera complété sur le Moodle au fur et à mesure des lectures.

Monitorat de programme

Le département d'informatique offre un service de monitorat gratuit s'adressant plus particulièrement aux étudiant.e.s du baccalauréat et du certificat en informatique. Il concerne principalement les cours de base comme INF1070, INF1120, INF1132, INF2120 et INF2171, mais, selon la connaissance du moniteur ou de la monitrice, un support dans d'autres cours peut également être offert.

Objectifs. Permettre aux étudiant.e.s de :

- Bénéficier d'un encadrement par les pairs ;
- Recevoir un suivi personnalisé en cas de difficulté ;
- Profiter d'un soutien supplémentaire à la matière vue en classe ;
- Obtenir un support technique sur les technologies, les outils, les bibliothèques et les cadriciels utilisés dans les cours (installation, configuration, utilisation)

Informations.

- Voir https://info.uqam.ca/aide/ pour la grille horaire et tous les détails
- Le service est généralement disponible à partir de la deuxième semaine
- D'autres plages horaires pourraient être ajoutées en cours de session selon les besoins
- Clavardage en direct : ~monitorat-de-programme (Mattermost)

Politique d'absence aux examens

Reprise d'examen. L'autorisation de reprendre un examen en cas d'absence est de **caractère exceptionnel**. Pour obtenir un tel privilège, l'étudiant-e doit avoir des motifs sérieux et bien justifiés.

Conflits d'horaire. Il est de la responsabilité de l'étudiant.e de ne pas s'inscrire à des cours qui sont en conflit d'horaire, tant en ce qui concerne les séances de cours ou d'exercices que les examens. **De tels conflits d'horaire ne constituent pas un motif justifiant une demande d'examen de reprise.**

Procédure. L'étudiant.e absent.e lors d'un examen doit, dans les cinq (5) jours ouvrables suivant la date de l'examen, présenter une demande de reprise en utilisant le formulaire prévu, disponible sur http://info.uqam.ca/repriseexamen/.

Pièces justificatives. Dans le cas d'une absence pour raison médicale, l'étudiant.e doit joindre un certificat médical original et signé par le médecin décrivant la raison de l'absence à l'examen. Les dates d'invalidité doivent être clairement indiquées sur le certificat. Une vérification de la validité du certificat pourrait être faite. Dans le cas d'une absence pour une raison non médicale, l'étudiant.e doit fournir les documents originaux expliquant et justifiant l'absence à l'examen ; par exemple, lettre de la Cour en cas de participation à un jury, copie du certificat de décès en cas de décès d'un proche, etc. Toute demande incomplète sera refusée. Si la direction du programme d'études de l'étudiant.e constate qu'un.e étudiant.e a un comportement récurrent d'absence aux examens, l'étudiant.e peut se voir refuser une reprise d'examen.

Pour plus d'informations. Consulter la page http://info.uqam.ca/politiques.

Règlement numéro 18 sur les infractions de nature académique (extraits)

Tout acte de plagiat, fraude, copiage, tricherie ou falsification de document commis par une étudiante, un étudiant, de même que toute participation à ces actes ou tentative de les commettre, à l'occasion d'un examen ou d'un travail faisant l'objet d'une évaluation ou dans toute autre circonstance, constituent une infraction au sens de ce règlement.
La liste non limitative des infractions est définie comme suit :

- la substitution de personnes ;
- l'utilisation totale ou partielle du texte d'autrui en la faisant passer pour sien ou sans indication de référence ;
- la transmission d'un travail pour fins d'évaluatiion alors qu'il constitue essentiellement un travail qui a déjà été transmis pour fins d'évaluation académique à l'Université ou dans une autre institution d'enseignement, sauf avec l'accord préalable de l'enseignante, l'enseignant ;
- l'obtention par vol, manoeuvre ou corruption de questions ou de réponses d'examen ou de tout autre document ou matériel non autorisés, ou encore d'une évaluation non méritée ;
- la possession ou l'utilisation, avant ou pendant un examen, de tout document non autorisé ;
- l'utilisation pendant un examen de la copie d'examen d'une autre personne ;
- l'obtention de toute aide non autorisée, qu'elle soit collective ou individuelle ;
- la falsification d'un document, notamment d'un document transmis par l'Université ou d'un document de l'Université transmis ou non à une tierce personne, quelles que soient les circonstances ;
- la falsification de données de recherche dans un travail, notamment une thèse, un mémoire, un mémoire-création, un rapport de stage ou un rapport de recherche ;
- Les sanctions reliées à ces infrations sont précisées à l'article 3 du Règlement no 18.

Les règlements concernant le plagiat seront strictement appliqués. Pour plus de renseignements :

- http://www.infosphere.uqam.ca/rediger-un-travail/eviter-plagiat
- http://r18.uqam.ca/

Politique no 16 visant à prévenir et combattre le sexisme et les violences à caractère sexuel

Les violences à caractère sexuel se définissent comme étant des comportements, propos et attitudes à caractère sexuel non consentis ou non désirés, avec ou sans contact physique, incluant ceux exercés ou exprimés par un moyen technologique, tels les médias sociaux ou autres médias numériques. Les violences à caractère sexuel peuvent se manifester par un geste unique ou s'inscrire dans un continuum de manifestations et peuvent comprendre la manipulation, l'intimidation, le chantage, la menace implicite ou explicite, la contrainte ou l'usage de force.
Les violences à caractère sexuel incluent, notamment :

- la production ou la diffusion d'images ou de vidéos sexuelles explicites et dégradantes, sans motif pédagogique, de recherche, de création ou d'autres fins publiques légitimes ;
- les avances verbales ou propositions insistantes à caractère sexuel non désirées ;
- la manifestation abusive et non désirée d'intérêt amoureux ou sexuel ;
- les commentaires, les allusions, les plaisanteries, les interpellations ou les insultes à caractère sexuel, devant ou en l'absence de la personne visée ;
- les actes de voyeurisme ou d'exhibitionnisme ;
- le (cyber) harcèlement sexuel ;
- la production, la possession ou la diffusion d'images ou de vidéos sexuelles d'une personne sans son consentement ;
- les avances non verbales, telles que les avances physiques, les attouchements, les frôlements, les pincements, les baisers non désirés ;
- l'agression sexuelle ou la menace d'agression sexuelle ;
- l'imposition d'une intimité sexuelle non voulue ;
- les promesses de récompense ou les menaces de représailles, implicites ou explicites, liées à la satisfaction ou à la non-satisfaction d'une demande à caractère sexuel.

Pour consulter la politique no 16

https://instances.uqam.ca/wp-content/uploads/sites/47/2018/05/Politique_no_16.pdf

Pour obtenir de l'aide, faire une divulgation ou une plainte

Bureau d'intervention et de prévention en matière de harcèlement
514-987-3000, poste 0886

Pour obtenir la liste des services offerts à l'UQAM et à l'extérieur de l'UQAM

https://harcelement.uqam.ca

Soutien psychologique (Services à la vie étudiante)

514-987-3185
Local DS-2110

CALACS Trêve pour Elles – point de services UQAM

514 987-0348
calacs@uqam.ca
http://trevepourelles.org

Service de la prévention et de la sécurité

514-987-3131

Politique no 44 d'accueil et de soutien des étudiant.e.s en situation de handicap

Politique. Par sa politique, l'Université reconnait, en toute égalité des chances, sans discrimination ni privilège, aux étudiant.e.s en situation de handicap, le droit de bénéficier de l'ensemble des ressources du campus et de la communauté universitaire, afin d'assurer la réussite de leurs projets d'études, et ce, dans les meilleures conditions possibles. L'exercice de ce droit est, par ailleurs, tributaire du cadre réglementaire régissant l'ensemble des activités de l'Université.

Responsabilité de l'étudiant.e. Il incombe aux étudiant.e.s en situation de handicap de rencontrer les intervenant.e.s (conseiller.ère.s à l'accueil et à l'intégration du Service d'accueil et de soutien des étudiant.e.s en situation de handicap, professeur.e.s, chargé.e.s de cours, direction de programmes, associations étudiantes concernées, etc.) qui pourront faciliter leur intégration à la communauté universitaire ou les assister et les soutenir dans la résolution de problèmes particuliers en lien avec les limitations entraînées par leur déficience.

Service d'accueil et de soutien aux étudiant.e.s en situation de handicap. Le Service d'accueil et de soutien aux étudiant.e.s en situation de handicap (SASESH) offre des mesures d'aménagement dont peuvent bénéficier certains étudiant.e.s. Il est fortement recommandé aux de se prévaloir de ces services afin de réussir ses études, sans discrimination. Pour plus d'information, visiter le site de ce service : https://vie-etudiante.uqam.ca/etudiant-situation-handicap/nouvelles-ressources.html et celui de la politique institutionnelle d'accueil et de soutien aux étudiant.e.s en situation de handicap : https://instances.uqam.ca/wp-content/uploads/sites/47/2018/05/Politique_no_44.pdf
Il est important d'informer le SASESH de votre situation le plus tôt possible :

- En personne : 1290, rue Saint-Denis, Pavillon Saint-Denis, local AB-2300
- Par téléphone : 514 987-3148
- Par courriel : situation.handicap@uqam.ca
- En ligne : https://vie-etudiante.uqam.ca/