COORDONNATEUR		BÉGIN, Guy	begin.guy@uqam.ca	(514) 987-3000 4081	PK-4825
GROUPE	40	GINGRAS, Éric	gingras.eric@uqam.ca	(514) 987-3000 3699	PK-4115

Jeudi, de 18h00 à 21h00 (cours) – Jeudi, de 21h00 à 23h00 (ateliers)

DESCRIPTION

Sensibiliser les étudiants aux différents aspects de la fiabilité et de la sécurité des systèmes informatiques. Introduire les techniques permettant d'assurer la fiabilité et la sécurité des processus. Fiabilité d'équipements et de logiciels. Procédures de sauvegarde et de recouvrement. Redondance. Tolérance aux défaillances et aux erreurs. Menaces à la sécurité: virus, imposteur, espion. Cryptologie. Authentification. Sécurité des systèmes répartis. Forteresse (firewall) contre intrusions. Travaux en laboratoire.

INF3105 Structures de données et algorithmes

OBJECTIF

Spécifique : Les compétences développées dans le cadre de ce cours rendront l'étudiant capable de :

- ❏ Définir et mettre en contexte les principaux objectifs et services de sécurité informatique, tels que *confidentialité, intégrité, authentification.*
- ❏ D'expliquer la fonction des principaux mécanismes de sécurité: chiffrage, hachage, signature, échange de clés.
- ❏ D'expliquer la fonction de protocoles cryptographiques courants utilisés en sécurité informatique.
- ❏ De distinguer les techniques à clé publique et à clé secrète. De reconnaître les vulnérabilités de systèmes informatiques.
- ❏ De définir les concepts importants en fiabilité informatique: fautes, défaillances, erreurs, fiabilité, disponibilité.
- ❏ De distinguer les paramètres probabilistes utilisées en fiabilité: MTTF, MTTR, MTBF.
- ❏ D'expliquer certaines techniques permettant d'améliorer la fiabilité: évitement de fautes, tolérance aux fautes et suppression de fautes.
- ❏ De pouvoir mettre en œuvre les mécanismes des langages de programmation visant à assurer la fiabilité des logiciels.

Ateliers en laboratoires

La séance de laboratoire prévue à l'horaire permettra aux étudiants de mettre en pratique un bon nombre des notions importantes apprises au cours. Les travaux pratiques à réaliser pourront prendre diverses formes selon la nature des concepts à expérimenter : exercices théoriques, programmes à réaliser, expérimentation avec des applications, etc.

Ces activités constituent une composante essentielle du cours et doivent être réalisées avec toute la rigueur et l'application nécessaires à leur réussite. On prévoit une dizaine de travaux à réaliser durant la session.

ÉVALUATION

Description sommaire	Date	Pondération
Examen partiel	Vendredi 26 février 2010 – 18h00 à 20h00	35%
Travaux pratiques		30%
Examen final	Vendredi 23 avril 2010 – 18h00 à 20h00	35%

Remise des TPs

Pour les TPs de type exercices, vous devez rendre une version ASCII, PostScript, ou PDF de vos réponses. Pour les TPs de type programmes, vous devez rendre le code source, l'éxécutable (paramètres d'exécution), de même que toutes les informations auxiliaires nécessaires (par ex., pages man et fichiers README). Assurez-vous que les programmes pourront être recompilés sans erreurs.

Les travaux et rapports doivent être **imprimés** par les étudiants et remis (au professeur) en classe ou au laboratoire, au début de la séance suivante.

Ce qui est recherché dans un TP de type programme

Lorsqu'un TP est noté, en plus de la pure fonctionnalité, nous recherchons la simplicité, la clarté, l'élégance et une documentation adéquate. Voici un aperçu de la pondération typique utilisée pour évaluer un programme :

- ❏ Programme correct (respect de l'énoncé) – 60%
- ❏ Commentaires, facilité de lecture, présentation – 20%
- ❏ Clarté de la sortie – 10%
- ❏ Documentation (README, page man, etc.) – 10%

Un programme qui ne se compile pas ne peut recueillir qu'un maximum de 30% de la valeur accordée au

programme.

Examens et plagiat

Les deux examens sont à documentation limitée.

Les règlements concernant le plagiat seront strictement appliqués. Pour plus de renseignements, veuillez consulter les sites suivants : **http://www.sciences.uqam.ca/decanat/note_integrite.doc**

et **http://www.bibliotheques.uqam.ca/recherche/plagiat/index.html**

Retards

Une pénalité de retard de 10% par jour ouvrable sera appliquée sur les travaux remis après les dates prévues. Un travail remis en retard sera corrigé comme normalement, après quoi la pénalité sera déduite du résultat. Il est de la responsabilité de l'étudiant de se faire des copies de ses travaux.

Politique d'absence aux examens

Un étudiant absent à un examen se verra normalement attribuer la note zéro pour cet examen. Cependant, si l'étudiant était dans l'impossibilité de se présenter à l'examen pour un motif valable, certains arrangements pourront être pris avec son enseignant. Pour ce faire, l'étudiant devra présenter à son enseignant l'un des formulaires prévus à cet effet accompagné des pièces justificatives appropriées (par ex., attestation d'un médecin que l'étudiant était dans l'impossibilité de se présenter à l'examen pour des raisons de santé, lettre de la Cour en cas de participation à un jury).

Une absence pour cause de conflit d'horaires d'examen n'est pas considérée comme un motif valable d'absence, à moins d'entente préalable avec la direction du programme et l'enseignant durant la période d'annulation des inscriptions avec remboursement : tel qu'indiqué dans le guide d'inscription des étudiants, il est de la responsabilité d'un étudiant de ne s'inscrire qu'à des cours qui ne sont pas en conflit d'horaire.

Pour plus de détails sur la politique d'absence aux examens du Département d'informatique et pour obtenir les formulaires appropriés, consultez le site web suivant :
http://www.info.uqam.ca/enseignement/reglements/politique-dabsence-aux-examens

CONTENU

Introduction et notions préliminaires

- ❏ Problématique d'ensemble de la qualité et de la sûreté de fonctionnement d'un système informatique.
- ❏ Probabilité et statistiques, analyse combinatoire, notion d'entropie, construction de logiciels, principes et fonctionnement des réseaux.

Sécurité informatique

- ❏ Problématique de la sécurité.
- ❏ Sécurité informatique vs sécurité de fonctionnement (innocuité).
- ❏ Menaces, vulnérabilités, attaques, préjudice, contrôles.
- ❏ Objectifs de sécurité : confidentialité, authenticité, intégrité, disponibilité.
- ❏ Mécanismes sécuritaires classiques et modernes : chiffrage symétrique et asymétrique, hachage, fonctions à sens unique. Modes d'opération.
- ❏ Protocoles sécuritaires : authentification, échange de clés, signature. Notion de confiance.
- ❏ Sécurité des systèmes : contrôle d'accès : objets, sujets. Mots de passe. Sécurité des programmes : virus, chevaux de Troie.
- ❏ Applications sécuritaires.

Fiabilité des systèmes informatiques

- ❏ Problématique de la fiabilité des systèmes informatiques.
- ❏ Causes : fautes, défaillances, erreurs.
- ❏ Fiabilité de système, de matériel, de logiciel : MTTF, MTTR, MTBF.
- ❏ Critères de sûreté de fonctionnement : fiabilité, disponibilité, innocuité, maintenabilité, testabilité.
- ❏ Mécanismes de contrôle : tolérance aux fautes, suppression des fautes, conception pour la fiabilité.
- ❏ Modélisation de la fiabilité, disponibilité.

Processus et méthodes

- ❏ Méthodologies et recommandations (pratiques d'excellence).
- ❏ Gestion de la qualité et de la sécurité.

RÉFÉRENCES

V R Amoroso, Edward G. – *Fundamentals of Computer Security Technology* – **Prentice Hall, 1994**

V R Amoroso, Edward G. – *Intrusion Detection : An Introduction to Internet Surveillance, Correlation, Trace Back, Traps, and Response.* – **Intrusion.net Books, 1999**

V R Bon – *Fiabilité des systèmes : méthodes mathématiques* – **Masson, Paris, 1995**

V R Denning, Dorothy – *Cryptography and Data Security* – **Addison-Wesley, 1984**

V R Fournier – *Fiabilité du logiciel : concepts, modélisations, perspectives* – **Hermes, Paris, 1993**

V R Garfinkel, Simson et Spafford, Gene – *Practical Unix and Internet Security* – **2e édition, O'Reilly & Associates, 1996**

V R Lyu, éd. – *Handbook of Software Reliability Engineering* – **IEEE Computer Society Press / McGraw-Hill, Los Alamitos (Calif.), NewYork, Montréal, 1996**

V R Motet, Geffroy – *Sûreté de fonctionnement des systèmes informatiques* – **InterÉditions/Dunod, Paris, 1998**

V R Mukhedkar, Sevestre, Bretault – *Aspects modernes de la fiabilité* – **Presses de l'Université de Montréal, Montréal, 1974**

V R Musa, Iannino, Okumoto – *Software Reliability: Measurement, Prediction, Application* – **McGraw-Hill Professional ed, New York, Montréal, 1990**

V R Pfleeger, Charles P. – *Security in Computing* – **3e édition, Prentice Hall, 2002**

V R Rook, éd. – *Software Reliability Handbook* – **Elsevier Applied Science, London, 1990**

V R Russel, D. et Gangemi, G. – *Computer Security Basics* – **O'Reilly & Associates, 1991**

V R Sabnis – *VLSI Reliability* – **Academic Press, San Diego, Calif.; Toronto, 1990**

V R Schneier, Bruce – *Cryptographie appliquée* – **2e édition, Vuibert, 1996**

V R Seeger, Karl A, VonStorch, William R. et Icove, David J. – *Computer Crime: A Crime-Fighter's Handbook* – **O'Reilly & Associates, 1995**

V R Siewiorek, Swarz – *Reliable Computer Systems: Design and Evaluation* – **2e édition, Digital Press, Bedford, Mass., 1992**

V R Siewiorek, Swarz – *The Theory and Practice of Reliable System Design* – **Digital Press, Bedford, Mass., 1982**

V R Stallings, William – *Network and Internetwork Security, Principles and Practice* – **Prentice Hall, 1995**

V R Stinson, Douglas R. – *Cryptographie, Théorie et pratique* – **Vuibert, 1995**

V R Zémor, Gilles – *Cours de cryptographie* – **Cassini, 2000**

A : article – C : comptes rendus – L : logiciel – N : notes – R : revue – S : standard – U : uri – V : volume

C : complémentaire – O : obligatoire – R : recommandé