

GROUPE 20 BÉGIN, Guy begin.guy@uqam.ca (514) 987-3000 4081 PK-4825

Mardi, de 18h00 à 21h00

DESCRIPTION Principes et concepts fondamentaux de la sécurité des systèmes informatiques. Principaux services: confidentialité, intégrité, disponibilité, authentification, non répudiation, contrôle d'accès. Typologie des attaques: fuites, modifications d'information, privations de service. Mécanismes sécuritaires modernes: systèmes de chiffrement symétriques et asymétriques; fonctions de hachage; génération pseudo-aléatoire. Protocoles sécuritaires: authentification, signature, échange et gestion de clés. Sécurité des systèmes centralisés et des systèmes répartis: politiques et modèles de sécurité; contrôle d'accès; rôles et privilèges. Sécurité des programmes: virus, chevaux de Troie. Contre-mesures: journalisation, audits; détection d'intrusion; filtrage; mécanismes de recouvrement. Analyse de risque. Éducation des usagers. Considérations légales, politiques et éthiques.

OBJECTIFS Avec la croissance fulgurante que connaît le monde des télécommunications, entraînée par la locomotive Internet et stimulée par la pénétration des technologies de transmission sans fil, la problématique de la sécurité des données et des processus prend de nos jours une importance cruciale. On abordera dans ce cours le très vaste sujet de la sécurité informatique, en s'intéressant aux principes fondamentaux, aux mécanismes permettant d'assurer des services de sécurité, de même qu'aux applications concrètes rencontrées dans les derniers déploiements technologiques. Le cours vise de prime abord à sensibiliser l'étudiant à la problématique de la sécurité dans un système informatique. Par la suite, par l'étude des principaux problèmes de sécurité et de leurs solutions possibles, on sera à même d'apprécier la complexité inhérente qui sous-tend la guerre perpétuelle que se livrent bons et méchants dans le monde de l'information électronique.

- Les compétences développées dans le cadre de ce cours rendront l'étudiant capable de:
- Définir des services de sécurité informatique tels que *confidentialité, intégrité, non-répudiation, authentification*.
- Énoncer les principes fondamentaux qui gouvernent l'établissement de services sécuritaires.
- Décrire et expliquer le fonctionnement des principaux algorithmes cryptographiques pour le chiffrement, le hachage, la signature électronique.
- Décrire les caractéristiques des systèmes de chiffrement à clé publique et à clé secrète.
- Mettre en œuvre des mécanismes de sécurité comme le chiffrement, la signature, le hachage.
- Décrire des protocoles cryptographiques courants utilisés pour la sécurité informatique.
- Effectuer une analyse de risque, en fonction d'un contexte de fonctionnement spécifique et d'hypothèses sur les menaces possibles.
- Identifier les particularités des menaces contre la sécurité selon le contexte centralisé ou décentralisé d'utilisation.
- Proposer des contre-mesures selon les menaces envisagées.

ÉVALUATION	Description sommaire	Date	Pondération
	Devoirs	périodiques	10%
	Travaux pratiques	périodiques	25%
	Travail de session	voir calendrier ci-bas	30%
	Examen final	fin de session	35%

Devoirs (10%)

Régulièrement au cours de la session, des séries d'exercices ou de programmes à réaliser en devoir *par équipes de deux* seront soumis aux étudiants. Typiquement, il y a deux devoirs avec environ deux semaines entre la soumission et la remise. Un sous-ensemble (inconnu à l'avance) des exercices pourront être retenus pour être notés.

Les énoncés des devoirs seront distribués par l'intermédiaire du site Web du cours, qui comportera également une foule d'autres informations utiles (et parfois nécessaires) pour le cours.

Les programmes remis **doivent** comprendre une documentation complète et suffisamment de cas de test pour démontrer leur fonctionnement correct. Tous les fichiers **doivent** contenir une en-tête comprenant les noms des auteurs, la date, les instructions de compilation et de lien, et toute autre information pertinente telle que des références bibliographiques.

Il n'y a pas de format pré-établi pour les documents à remettre, mais la qualité de présentation et de rédaction est importante. Je n'aime pas particulièrement les torchons et tend à les noter en conséquence. Une réponse ou un raisonnement illisibles sont forcément mauvais.

Travaux pratiques (25%)

Occasionnellement au cours de la session, des travaux pratiques permettront aux étudiants de mettre en pratique et de vérifier expérimentalement certains des concepts présentés en classe. Les travaux, qui devront être réalisés en *équipes de deux*, toucheront à différents sujets en sécurité informatique: configuration et mise en oeuvre de protocoles sécuritaires, explorations de vulnérabilités classiques, etc. Il pourra y avoir de la programmation à effectuer, mais pas de développements majeurs.

Travail de session (projet) (30%)

Comme nous aborderons un domaine beaucoup plus vaste que ce qu'il est possible de couvrir durant le temps limité qui est alloué au cours, un travail de longue haleine, réalisé dans le cadre du cours, vous permettra d'en approfondir un aspect particulier à votre choix. Ce travail peut prendre diverse formes: compte-rendu de lectures, application pratique de notions vues en classe, réalisation de logiciel ou de matériel, etc. Le produit fini devra de toute façon comporter un rapport, qui rendra compte de votre travail et permettra de démontrer ce que vous avez pu apprendre au-delà de ce qui est couvert en classe.

Vous devrez d'abord sélectionner un sujet, qui sera ensuite approuvé par le professeur.

Pour faire ce choix, on peut:

- penser à un aspect de l'informatique ou des télécommunications et de le relier au concept de sécurité
- discuter avec des collègues étudiants ou de travail pour des suggestions
- songer à l'amélioration de la sécurité d'un système sur lequel vous travaillez
- consulter un (des) articles intéressants sur la sécurité

Les principales revues traitant de sécurité informatique sont: Computers & Security, Journal of Computer Security, mais on trouve des articles sur le sujet dans plusieurs autres revues. Les principales conférences sont Crypto et Eurocrypt (pour la cryptographie), Symposium on Research in Security and Privacy, National Computer Security Conference, et Annual Computer Security Applications Conference.

Quelques suggestions de sujets (liste non-exhaustive):

- Anonymat, vie privée et confidentialité
- Aspects sécuritaires de systèmes d'exploitation connus
- Authentification biométrique
- Authentification dans un environnement distribué
- Cartes à puce pour la sécurité
- Éthique informatique
- Gestionnaires de licences pour logiciels
- Pares-feu, contrôle d'accès par listes
- Prévention et détection d'intrusion avancée
- Sécurité et bases de données
- Sécurité et commerce électronique
- Sécurité et facturation de services
- Sécurité et réseaux sans fil/ad hoc
- Stéganographie, copyright et protection contre la copie
- Virus
- Nuisances (pourriels, adware, etc.)

Principaux jalons et éléments à remettre:

- Semaine 4: Vous devez avoir fait le choix définitif du sujet. Vous devez remettre un document de 2 à 3 pages expliquant ce que vous voulez faire et pourquoi. Vous devez fournir plusieurs sources bibliographiques et décrire comment vous comptez vous y prendre pour compléter le projet. (10 % de la note du projet)
- Semaine 8: Votre projet doit être bien avancé. Vous devez remettre un plan **détaillé** ou une spécification de design complète. Il importe de préciser ce que vous faites, comment et quels sont les résultats spécifiques que vous attendez. De plus, vous devez justifier la pertinence de votre travail et indiquer comment votre travail peut être d'intérêt général. (30 % de la note du projet)
- Semaine 13 : Séance de présentations par affiches. Chaque étudiant prépare et présente en quelques minutes une affiche (poster) décrivant de façon synthétique son travail. L'évaluation se fera par les pairs et par le professeur, à parts égales (20% de la note du projet: 10% note du groupe; 10% note du professeur)
- Semaine 14: Remise du rapport final. Le produit fini doit être d'assez bonne qualité pour être soumis à un magazine ou à votre supérieur au travail. (40% de la note du projet)

Examen final (35%)

Examen à **livre fermé**, portant sur l'ensemble de cours. La note de l'examen final doit être égale ou supérieure à 50%. Si ce seuil n'est pas atteint, la mention échec sera automatiquement attribuée au cours et ce, quelles que soient les notes obtenues dans les travaux pratiques.

Prenez note que la correction des exercices et examens tient abondamment compte des développements. Il est donc avantageux d'**exposer votre travail**. Une réponse correcte obtenue au terme d'un raisonnement invalide 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.

Les règlements de l'UQAM concernant le plagiat seront strictement appliqués. 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 débogage.

En cas de doute sur l'originalité des travaux, un test oral pourra être exigé. En cas de plagiat, les sanctions suivantes seront appliquées:

- première offense : tous les étudiants impliqués dans le plagiat se verront attribuer la note zéro pour ce travail;
- deuxième offense: tous les étudiants impliqués dans le plagiat se verront attribuer un échec pour le cours.

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.

CONTENU

Introduction: Problématique de la sécurité: confidentialité, intégrité, disponibilité, authentification, non-répudiation, contrôle d'accès. Vulnérabilités, menaces à la sécurité et attaques. Attaques conduisant à des fuites d'information (divulgaration de contenu, analyse de trafic), à des modification d'information (modifications de contenu ou d'ordre des messages, reprises de messages), à des privations de service (retard de messages, destruction). Notion de confiance.

Techniques de base en sécurité: Terminologie. Techniques de chiffrage. Mécanismes de base: transposition, permutation. Caractérisation des systèmes de chiffrage. Cryptanalyse et attaques. Notions de base fondamentales: entropie, redondance

Mécanismes sécuritaires modernes: Systèmes de chiffrage symétriques (clé privée: DES, IDEA) et asymétriques (clé publique: Diffie-Hellman, RSA, DSA). Éléments de théorie des nombres. Complexité de calcul. Fonctions à sens unique. Fonctions de hachage (MD5, SHA). Hachage avec clé secrète. Intégrité des données et authentification de message. Génération pseudo-aléatoire. Modes de chiffrage: en blocs, continu, chaînage de blocs chiffrés.

Protocoles sécuritaires: Identification et authentification. Protocole: signature, authentification mutuelle. Échange et gestion de clés. Tiers de confiance. Authentification par défi et réponse. Protocoles sans transfert de connaissances. Infrastructures d'authentification et de distributions de clés: X.509. Certificats.

Exemples d'applications sécuritaires: PGP, IPsec.

Sécurité des systèmes centralisés: Politiques et modèles de sécurité: sécurité multi-niveaux, étiquetage. Contrôle d'accès: objets, sujets. Mots de passe. Rôles et privilèges. Politiques et matrices de contrôle d'accès. Treillis descriptif. Sécurité des programmes: virus, chevaux de Troie, canaux subliminaux.

Sécurité des systèmes répartis et de réseaux: Menaces spécifiques: écoute illicite, imposture, déni de service, brouillage. Caractéristiques des médiums de transmission. Gestion de la confiance. Autorisation décentralisée. Pare-feu. Réseaux privés virtuels.

Contre-mesures: Journaux de bord (logs) et audits. Détection d'intrusion. Filtrage. Mécanismes de recouvrement. Analyse de risque. Principes et politiques de sécurité. Éducation des usagers

Considérations légales, politiques et éthiques: Hackers et crackers. Ingénierie sociale. Crime informatique. Accès légal à l'information et consignation de clés. Restrictions à l'exportation.

RÉFÉRENCES

U O <http://www.moodle.uqam.ca/>

V R **SÉCURITÉ EN GÉNÉRAL**

V R Charles P. Pfleeger – *Security in Computing* – 2nd Ed. Prentice Hall, Inc., 1997.

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

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

V R D. Russell and G. Gangemi, Sr. – *Computer Security Basics O* – 'Reilly & Associates, 1991.

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

- VR Edward Amoroso – *Intrusion Detection: An Introduction to Internet Surveillance, Correlation, Trace Back, Traps, and Response* – *Intrusion.net Books*, 1999.
- VR Karl A. Seeger, William R. VonStorch, and David J. Icové – *Computer Crime: A Crime-Fighter's Handbook* – *O'Reilly & Associates*, 1995.
- VR Simson Garfinkel et Gene Spafford – *Practical Unix and Internet Security* – (2nd edition), *O'Reilly & Associates*, 1996.
- VR **CRYPTOLOGIE EN GÉNÉRAL**
- VR Bruce Schneier – *Applied Cryptography* – *Second Edition*, *John Wiley and Sons*, 1996.
- VR Douglas R. Stinson – *Cryptography, Theory and Practice* – *CRC Press, Inc.*, 1995.
- VR Alan Konheim – *Cryptography: A Primer* – *John Wiley and Sons*, 1981.
- VR Wayne Patterson – *Mathematical Cryptography for Computer Scientists and Mathematicians* – *Rowman and Littlefield*, (c)1987.
- VR Abraham Sinkov – *Elementary Cryptanalysis: A Mathematical Approach* – *The Mathematical Association of America*, 1966.
- VR Peter Wayner – *Disappearing Cryptography* – *Academic Press*, 1996.
- VR Carl Meyer and Stephen Matyas – *Cryptography: A New Dimension in Computer Data Security* – *John Wiley and Sons*, 1982.
- VR **CONNEXE ET INTÉRESSANT**
- VR David Kahn – *The Codebreakers* – *Second Edition*, *Macmillan*, 1996.
- VR Helen Fouché Gaines – *Cryptanalysis: a Study of Ciphers and their Solution* – *Dover Publications*, 1956.
- VR Peter G. Neumann – *Computer Related Risks*, – *Addison-Wesley/ACM Press*, 1995. (reprinted with corrections, Jan 1995).
- VR Charlie Kaufman, Radia Perlman, Mike Speciner – *Network Security, Private Communication in a Public World* – *Prentice Hall, Inc.*, 1995.
- VR Katie Hafner and John Markoff – *Cyberpunk* – *Simon & Schuster*, 1991.
- VR Simson Garfinkel – *PGP, Pretty Good Privacy* – *O'Reilly & Associates*, 1995.
- VR Lance J. Hoffman, – *Rogue Programs: Viruses, Worms, and Trojan Horses* – *Van Nostrand Reinhold*, 1990.
- VR National Research Council – *Computers at Risk: Safe Computing in the Information Age* – *National Academy Press*, 1991.
- VR Donn Parker – *Crime by Computer* – *Charles Scribner's Sons*, 1976.
- VR **AUTRES LECTURES**
- NR D'autres documents pourront être soumis pour lecture durant la session. La liste sera tenue à jour sur le site Web du cours.

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

C : complémentaire – O : obligatoire – R : recommandé