Université Saint-Joseph
Faculté d'Ingénierie
Institut National des Télécommunications et de l'Informatique

Master en Systèmes et réseaux
Option Sécurité de l'Information

Master of Science in Systems and Networks
Cybersecurity Track

ماستر في الأنظمة والشبكات ـ فرع حماية ألمعلومات

Catalogue 2019-2020

Institut National des Télécommunications et de l'Informatique
Campus des Sciences et Technologies, Mar Roukos, Liban
mél: inci@usj.edu.lb

Master en Systèmes et réseaux - Option Sécurité de l'Information

1 Objectifs et débouchés

L'objectif du Master en Systèmes et Réseaux - Option Sécurité de l'Information est de former des spécialistes sécurité maîtrisant les différentes techniques de sécurisation qui peuvent être utilisées dans les systèmes et les réseaux afin de protéger l'accès aux informations et de préserver la confidentialité, l'intégrité et la disponibilité des données.

La sécurité de systèmes et réseaux s'adresse à tous les acteurs de l'économie : entreprises (toutes tailles confondues), opérateurs, intégrateurs, sociétés de services,...

Plusieurs types de métiers peuvent être envisagés :

- Consultant de sécurité de l'information
- Responsable de sécurité
- Administrateur réseaux
- Expert technique
- Avant-vente (pre-sales)
- Chef de projet
- etc.

Un point essentiel de ce cursus est de former des professionnels de " terrain " sur le domaine de la sécurité, opérationnels dès leur sortie du Master; c'est pourquoi une bonne partie de la formation est consacrée à l'aspect pratique, par la mise en œuvre des thèmes abordés. Ce Master Professionnel comporte 120 crédits, répartis sur 4 semestres M1-1, M1- 2, M2-1 et M2-2.

2 Poursuite d'études

3 Admission

Admission en premier semestre du cursus Master (M11)

Sur dossier pour les candidats:

- titulaires d'une licence en Télécommunications ou en Informatique,
- titulaires d'un diplôme reconnu équivalent par la commission des équivalences de l'USJ.

Admission en troisième semestre du cursus Master (M13)

Sur dossier pour les candidats:

- titulaires d'une maîtrise ou d'un Master M1 en Systèmes et Réseaux ou en Télécommunications ou en Informatique,
- titulaires d'un diplôme d'ingénieur,
- titulaires d'un diplôme reconnu équivalent par la commission des équivalences de l'USJ.

La sélection sur dossier s'effectue dans la limite des places disponibles.

4 Compétences et résultats d'apprentissage niveau programme

A. An ability to detect, analyze and respond to cyberattacks in compter and network systems

B. An understanding of the legal and ethical issues related to securing information systems

C. An ability to integrate the acquired knowledge in cybersecurity to propose solutions for real world problems

D. An ability to collect, investigate and process digital evidence established at a crime scene tor effective recovery of information

E. An ability to continuously monitor, maintain, and enhance the protection of systems through widely accepted standards, procedures and policies

F. An ability to conduct risk and vulnerability assessments of existing systems

G. An ability to communicate effectively both in written and oral form

5 Prérequis de réussite

Pour obtenir son diplôme, chaque étudiant doit valider:

- 112.0 crédits Obligatoire
- 8.0 crédits Optionnelle fermée

6 Programme prévisionnel

2020, sem. 1

Code	Unité d'enseignement	Cr.	Type
026ADUNM1	Administration UNIX	6.0	Obligatoire
026AGREM1	Architecture et gestion des réseaux	6.0	Obligatoire
026GOSIM1	Gouvernance des systèmes d'information	2.0	Obligatoire
026MOREM1	Modélisation et optimisation des réseaux	6.0	Obligatoire
026NTIPM1	Nouvelles technologies pour réseaux IP	6.0	Obligatoire
026WSADM1	Windows system administration	4.0	Obligatoire

2020, sem. 2

Code	Unité d'enseignement	Cr.	Type
026BIGDM2	Big Data	4.0	Optionnelle fermée
026BLCHM2	Block chain	4.0	Optionnelle fermée
026COUNM2	Communications unifiées	4.0	Obligatoire
026CRASM2	Cryptographie et applications sécurisées	4.0	Obligatoire
026DRINM2	Droit informatique	2.0	Optionnelle fermée
026GEPRM2	Gestion de projets	2.0	Obligatoire
026INDTM2	Innovation's management and design	4.0	Optionnelle fermée
026INENM2	Introduction to entrepreneurship	2.0	Optionnelle fermée
026PRJ1M2	Projet 1	6.0	Obligatoire
026REFIM2	Réseaux sans fil	6.0	Obligatoire
026SDDCM2	Software defined data center	2.0	Optionnelle fermée

2021, sem. 1

Code	Unité d'enseignement	Cr.	Type
026DIFOM3	Digital forensics	4.0	Obligatoire
026GERIM3	Gestion des risques	2.0	Obligatoire
026ISSPM3	Information security - standards and best practices	4.0	Obligatoire
026ISASM3	Information systems administration and security	2.0	Obligatoire
026PIETM3	Piratage éthique	4.0	Obligatoire
026PRJ2M3	Projet 2	6.0	Obligatoire
026REESM3	Réseau d'entreprise sécurisé	4.0	Obligatoire
026SEREM3	Sécurité des infrastructures réseaux	4.0	Obligatoire

2021, sem. 2

Code	Unité d'enseignement	Cr.	Type
026STAGM4	Stage professionnel	30.0	Obligatoire

7 Liste des unités d'enseignement

026ADUNM1. Administration UNIX (6.0 Cr.)

Objectif. Initiation aux techniques d'administration et de sécurité d'un réseau de stations de travail ayant Unix pour système d'exploitation.

Contenu. Administration locale: Rôle d'un administrateur - Démarrage et arrêt - Ouverture d'une session - Gestion des utilisateurs - Gestion des processus - Gestion du disque - Sauvegarde et Compression - Gestion des imprimantes - Tâches périodiques - Fichiers de trace. Administration d'un réseau des stations Unix: Configuration d'un serveur réseau - Outils de base - DNS - NIS - NFS et Automount - Mail - Serveur Web et Proxy - DHCP - PPP - Sécurité - Optimisation et paramétrage. Systèmes d'exploitation de confiance (Trusted Solaris, SELinux)

026AGREM1. Architecture et gestion des réseaux (6.0 Cr.)

Objectif. Maîtriser l'architecture des réseaux de communications et les concepts de base relatifs.

Contenu. Rappel sur le modèle OSI et les fonctionnalités de chaque couche - Rappel sur les technologies niveau 2 et 3 utilisé dans les réseaux LAN, MAN et WAN (Ethernet/VLAN - WiFi - Frame Relay - ATM - IP - VPN, ...) - Architecture des réseaux d'entreprise au niveau LAN et WAN - Architectures des unités d'interfonctionnement - Techniques d'interconnexion au niveau 2 et aux niveaux supérieurs - Evolution des réseaux vers le large bande - Réseaux Gigabit - Techniques de gestion de la bande passante - Architecture des centres de données - les réseaux de stockage - le contrôle d'accès et le filtrage réseau - les zones de sécurité. Problématique de la gestion des réseaux - Syntaxe abstraite et codage des données de gestion - Protocoles CMIS/CMIP et SNMP - Structure des informations de gestion (SMI) - MIB standards et RMON.

026BIGDM2. Big Data (4.0 Cr.)

Objectif. Le cours présente les différents aspects théoriques et pratiques pour la gestion des données massives: Calcul distribué avec MapReduce, analyse des liens dans les graphes, PageRank, recherche des ensembles et sous-ensembles similaires, identification des communautés dans les graphes, Traitement des flots de données, les systèmes de recommendation et de classification, Detection des ensembles séparables (clustering).

Contenu. Introduction : Les enjeux des données massives, Calcul distribué, HPFS et MapReduce, Analyse des liens et PageRank, Ensembles similaires (MinHashing et Local Sensitive Hashing),

Sous-ensembles similaires (A-priori alogithm), Détection des communautés dans les graphes (clustering et BigClam), Traitement des flots de données, Systèmes de recommandation, Détection des ensembles séparables

026BLCHM2. Block chain (4.0 Cr.)

Objectif. The Blockchain technology is evolving fast and enabling businesses to create many types of applications beyond Fintech. The course aims to provide proof-of-knowledge in the Blockchain space, gain an in-depth understanding of Blockchain and its implementation while helping you apply your skills in any Blockchain applications.

Contenu. Introduction, distributed ledger technology, bitcoins, Keys and addresses, wallets, transactions, advanced transactions, Bitcoin network, Blockchain, mining and consensus, Business applications of block chains, crypto currency, Ethereum, Smart contract, decentralized applications, Blockchain application beyond the financial industry, Hyper-ledger, other DLTs, Advanced topics on Blockchain, Blockchain security, Blockchain-as-a-Service.

026COUNM2. Communications unifiées (4.0 Cr.)

Objectif. Ce cours couvre les standards de compression audio et vidéo qui constituent la partie majeure des flux multimédia, ainsi que les protocoles de transmission et de contrôle de ces flux. Le tout couronné par trois applications majeures : la téléphonie IP, la visioconférence et la diffusion vidéo (vidéo streaming).

Contenu.

026CRASM2. Cryptographie et applications sécurisées (4.0 Cr.)

Objectif. acquérir les connaissances nécessaires pour la sécurisation de l'information en utilisant la cryptographie.

Contenu. Services, Mécanismes et Techniques de sécurité - Algorithmes Symétriques, Asymétriques et Hash - Certificats - Mécanismes d'authentification, non-répudiation, confidentialité, intégrité et échanges de clés - Cartes à puces - TPs et TDs reprenant l'ensemble du cours.

026DIFOM3. Digital forensics (4.0 Cr.)

Objectif. Digital forensics is the practice of collecting, analyzing and reporting on digital data and events in a way that is legally admissible. It can be used in the detection and prevention of digital and cyber-crime and in any dispute where evidence is stored digitally. Digital forensics is simply the application of computer investigation and analysis techniques in the interests of determining potential legal evidence. Evidence might be sought in a wide range of computer crime or misuse, including but not limited to hacking, theft of trade secrets, theft of or destruction of intellectual property, and fraud.

Contenu. -The process of investigating cyber-crime, laws involved, and the details in seizing digital evidence - The different types of digital evidence, rules of evidence, digital evidence examination process, and electronic crime and digital evidence consideration by crime category - The roles of first responder, first responder toolkit, securing and evaluating electronic crime scene, conducting preliminary interviews, documenting electronic crime scene, collecting and preserving electronic evidence, packaging and transporting electronic evidence, reporting the crime scene - The process of investigating cyber and digital incidents such as hacking, e-fraud, data leakage, or evidences stored on digital media or devices - Log capturing techniques, log management, time synchronization, log capturing tools and SIEM solutions

026DRINM2. Droit informatique (2.0 Cr.)

Objectif. Le développement croissant de l'Informatique et de l'Internet a mis en évidence la nécessité de législation juridique alignée avec la technologie de l'information. Comment assurer la balance entre la technologie de l'Information et la législation informatique? Sommes-nous bien armés juridiquement et bien préparés face à l'évolution rapide de l'Internet? Le cours "Droit Informatique" expose les thèmes primordiaux et les problématiques essentielles de la législation de nos jours, en proposant une échelle de comparaison entre le Liban et les lois Européennes.

Contenu. 1) Le Droit Informatique - Contexte & Notions Générales 2) L'Actualité juridique au Liban - Ou sommes-nous par rapport à l'Europe? 3) La propriété intellectuelle au service des créations informatiques 4) Les Contrats - Négociation & Elaboration 5) La protection juridique & Droit pénal face à la criminalité informatique 6) La Signature Electronique - Enjeux & Application 7) La CNIL - Pourquoi & Comment ? 8) Les perspectives du Droit Informatique pour les années à venir.

026GEPRM2. Gestion de projets (2.0 Cr.)

Objectif. Le cours de " Project Management " permet aux étudiants de connaître les différentes phases d'un projet qui sont indispensables pour la bonne gérance de ce dernier. Ces phases se résument en : La planification, le développement du Schedule et le contrôle. De plus, plusieurs notions de Management seront abordées dans ce cours et qui sont reconnues comme étant les meilleures pratiques managériales pour la réussite d'un Project Manager.

Contenu. 1. Introduction au " Project Management " 2. Planification d'un projet 3. Schedule du projet 4. Ressources Humaines du projet 5. Management de la communication 6. Coût du projet 7. Contrôle du projet

026GERIM3. Gestion des risques (2.0 Cr.)

Objectif. Ce cours a pour objectif de présenter la gestion des risques de sécurité des systèmes d'information afin de sensibiliser à la gestion des risques, savoir que la gestion des risques est maitrisable, comprendre qu'il existe des méthodes pour analyser les risques et appréhender la mise en place d'un plan de gestion des risques. Contenu

Contenu. Concept de la gestion des risques - Processus de gestion des risques - bonnes pratiques pour la gestion des risques - principes de gestion des risques du SI - culture et communication - dépendance avec la stratégie et objectifs métiers - identification du risque - scenarios de risques - sensibilisation au niveau gestion des risques - notions de " capacity, appetite, tolerance " - différentes phases d'évaluation des risques - méthodes d'analyse des risques - définition et mise en œuvre des solutions - contrôle des risques

026GOSIM1. Gouvernance des systèmes d'information (2.0 Cr.)

Objectif. Comment améliorer l'efficacité et la productivité des entreprises? Comment aligner les technologies de l'Information avec les enjeux métier de l'organisation? Comment rentabiliser les investissements informatiques? Comment piloter les évolutions des systèmes d'information? Le cours "Gouvernance des SI" permet de répondre à l'ensemble de ces questions, en présentant une démarche d'amélioration continue de production informatique, enrichie par des retours d'expérience et des références du Marché Européen.

Contenu. La Gouvernance des SI: Concept, Enjeux, Bonnes Pratiques, Processus, Méthodes & Outils. ITIL: Vue d'Ensemble & Organisation, Vue détaillée sur la Démarche d'Industrialisation des Environnements, Implémentation pratique des processus, infrastructures et outils au sein des Entreprises. COBIT: Structure, domaines et processus, Application concrète & complémentarité avec les autres standards (ITIL, CMMI, et autres). L'Intégration de la Gouvernance des SI dans l'Approche globale de la Sécurité d'Entreprise. La Gouvernance des SI: Analyse & Réflexions sur la pérennité et sur l'évolution

026ISSPM3. Information security - standards and best practices (4.0 Cr.)

Objectif. The purpose of this course is to introduce students to the various IT security standards, best practices and guidelines. It tackles the different risk analysis standards and best practices, the design and implementation of security controls and the management of a security program within an institution.

Contenu. Security Policy - Organization of information security - Asset management - Human Resources security - Physical and Environmental security - Communication and operations management - Access control - Information Security incident Management - Business Continuity Management

026ISASM3. Information systems administration and security (2.0 Cr.)

Objectif.

Contenu.

026INDTM2. Innovation's management and design (4.0 Cr.)

Objectif. In a rapid changing and complicated world with fast evolving products and business models, innovation has become a must for every professional especially in engineering. Innovation and design thinking focuses on the leader's role as an innovator and facilitator of innovation. This course allows students to develop basic skills in innovation and creative problem solving. Innovation can be applied to any discipline, and a special focus would be to search for innovative solutions for daily social problems. Innovation is a practical transformation of ideas to new products, services, processes, systems and social interactions. It creates new added values that satisfy interest groups and drive sustainable growth, improve the quality of living and promote a sustainable society. Innovation isn't only technology; it develops in all the economy and society dimensions. (EFQM framework for Innovation). The term was created in 1980s at Stanford to characterize the approach designers, architects or artists use to solve problems. The approach is users' centered, focusing on their needs. Considering that the approach is based in the design world, it uses tools like look/ask/try and visual thinking to understand and communicate ideas. Even though Innovation and design thinking have been related to product design, they can be applied to all kind of problem solving including business modeling and processes.

Contenu.

026INENM2. Introduction to entrepreneurship (2.0 Cr.)

Objectif. Prepare the students to what it takes to create a startup.

Contenu. - Defining: Entrepreneurship - Innovation - Invention - Ideate - Generating business ideas - Identifying business opportunities - The tools: SWOT, PESTEL, business model canvas - Marketing & communication - Financials of the project - Feasibility Study & business plan - How to prepare the presentation / pitch

026MOREM1. Modélisation et optimisation des réseaux (6.0 Cr.)

Objectif. Dimensionner et analyser la topologie et les performances des réseaux en utilisant les outils de modélisation mathématique de la théorie des graphes, de la recherche opérationnelle et des processus stochastique.

Contenu. Cette UE introduit les fondements de la modélisation et le dimensionnement des réseaux en utilisant plusieurs outils théoriques comme les graphes, la recherche opérationnelle et les files d'attente. L'UE couvre les bases de la théorie des graphes, la représentation et le parcours des graphes, les problèmes classiques de la théorie des graphes comme l'arbre couvrant de poids minimal, le plus court chemin et les réseaux de transport, la manipulation et l'analyse des réseaux utilisant des librairies logicielles pour les graphes. L'UE introduit aussi la théorie de télétrafic,

l'utilisation des probabilités pour la modélisation du multiplexage et du trafic, les chaînes de Markov et leur application aux réseaux, les processus d'arrivées, les files d'attente de type M/M et leurs applications, l'optimisation et les programmes linéaires, les outils de résolution numérique des problèmes d'optimisation.

026NTIPM1. Nouvelles technologies pour réseaux IP (6.0 Cr.)

Objectif. Analyser l'interconnexion des réseaux dans l'Internet et l'évolution des protocoles

Contenu. Interconnexion des systèmes autonomes - Accords de transit et de peering - Point d'échange Internet - Principes du routage externe - Protocole BGP - Stratégies de routage BGP - Sécurité de routage dans l'Internet - Architecture MPLS - VPN MPLS - Ingénierie de trafic - Transition vers IPv6 - Auto-configuration IPv6 - Application double pile

026PIETM3. Piratage éthique (4.0 Cr.)

Objectif. Ce cours apprend à identifier des faiblesses dans le réseau en utilisant les mêmes méthodes que les "hackers": prise d'empreintes, énumération, exploitation et escalade de privilèges. Les étudiants apprendront également les contre-mesures à prendre, telles que les correctifs, pour atténuer les risques.

Contenu. Piratage : Classes des pirates, Anatomie d'une attaque, Test d'intrusion - Reconnaissance Passive - Balayage: Découverte des machines actives, Balayage des ports, Détection des systèmes d'exploitation, Test de vulnérabilités - Craquage des mots de passe - Enumération - Attaque Système : Gagner l'accès, Post-attaque - Attaques Réseaux : Les attaques par Déni de Service, Le reniflement du réseau, L'usurpation d'identité - Attaque sur les applications Web - Ingénierie sociale.

026PRJ1M2. Projet 1 (6.0 Cr.)

Objectif. Mise en application des connaissances acquises en 1ère année de Master.

Contenu.

026PRJ2M3. Projet 2 (6.0 Cr.)

Objectif. Implémentation d'une solution de sécurité

Contenu. Un mini-projet de 100 heures de travail personnel sur des thèmes liés à la sécurité. Exemples: Sécurisation d'une plateforme de recherche - Détection d'intrusion - Mise en place d'un pare-feu et des règles de filtrage en accord avec la politique de sécurité ...

026REESM3. Réseau d'entreprise sécurisé (4.0 Cr.)

Objectif. Maitriser le fonctionnement et le déploiement d'un réseau d'entreprise sécurisé.

Contenu. Les différentes technologies des pare-feu: Filtrage de paquets, filtrage applicatif (proxy), filtrage dynamique, filtrage de sessions. Analyse du contenu: lutte contre les SPAMs, protection contre les virus. Les systèmes de détection d'intrusion - Rappel sur l'architecture des réseaux d'entreprise - choix des technologies et dimensionnement des équipements de sécurisation: l'authentification centralisée, le SSO, Contrôle d'accès, NAC, les zones de sécurité, UTM, VPN (L2TP, IPsec, SSL) - Meilleur emplacement des différents dispositifs de sécurité. Travaux pratiques: Mise en place d'un pare-feu dans un réseau avec écriture des règles - Scan de ports avant et après la mise en place du pare-feu - IDS - Mettre en œuvre le proxy squid. Mise en œuvre de serveurs VPN - Etude de cas.

026REFIM2. Réseaux sans fil (6.0 Cr.)

Objectif. This course is intended to give a good overview of the topics and materials that are needed in the daily work of a wireless engineer.

Contenu. Partie 1. It focuses on 3G (3rd generation) mobile telephony, UMTS (Universal Mobile Telecommunications System), and on 4G (4th generation) also called LTE (Long Term Evolution). Whereas the 2G (2nd generation), GSM (Global System for Mobile Communications) is not part of this course and is only mentioned in few scenarios just for the sake of comparison with 3G.

Partie 2. La deuxième partie commence par une introduction de la nature du médium sans fil suivie par les différentes méthodes d'accès utilisées dans ces réseaux (exemples : ALOHA, les différents types de CSMA/CA). Etude de cas des méthodes d'accès des normes IEEE 802.11 et IEEE 802.15.4. Durant les séances pratiques les étudiants mettront en place différentes configurations de réseaux WiFi. Les aspects suivants seront abordés : SSID - association - répéteur - analyseur - redondance - VLAN - routage - NAT.

026SDDCM2. Software defined data center (2.0 Cr.)

Objectif. This course will focus on explaining how to extend the benefits of virtualization across the entire data center infrastructure components (networking, processing, storage) in the aim of delivering higher efficiency in service provisioning with better availability and security.

Contenu. Active components of a Datacenter - Traditional Data center technologies - Cloud computing and Virtualization(Concepts, Different Models, Technologies, Security) - Virtualization technologies(Systems virtualization, Storage virtualization, Network virtualization, Virtual network devices, SDN) - Converged Infrastructures - Hyper-Converged Infrastructures

026STAGM4. Stage professionnel (30.0 Cr.)

Objectif. Stage professionnel de 4 mois dans une entreprise sur un thème lié à la sécurité.

Contenu. Mission en entreprise d'une durée de 3 à 4 mois, conclue par la rédaction et la soutenance d'un mémoire professionnel.

026SEREM3. Sécurité des infrastructures réseaux (4.0 Cr.)

Objectif. Apprendre les techniques de Sécurité offertes par les équipements réseaux.

Contenu. Sécurité offerte par les équipements réseaux du marché: hub, commutateur, routeur, pare-feu, translation d'adresses - Spécificités de la sécurité Intranet - Sécurité téléphonie classique/PABX - Sécurité des réseaux radio-mobile, sans fils, multimédia sur IP, ... Disponibilité du réseau: Fonctions de redondance, protection physique et/ou logique contre les attaques - Offres de services à partir des VPNs. Travaux pratiques: Filtrage sur les routeurs - Mise en oeuvre d'un VPN IPSec entre routeurs.

026WSADM1. Windows system administration (4.0 Cr.)

Objectif. Understand the Microsoft Windows architecture, and master the management of a Microsoft Windows Server and its features, roles and services; all using a direct hands-on experience with the products and tools.

Contenu. - Fundamentals, covering PC and Server hardware architecture, Operating System, and Networking - Windows Server: Architecture of Operating System - Installation and Configuration - Configuring Network Services(DHCP, DNS, Routing, Remote Access, VPN) - Backup and Recovery - Security and Identity Management (Active Directory, Group Policy Management, Certificate Services, Federated Services, Network Access Control and Policy Management, Server Hardening) - Virtualization (Hyper-V) - Overview of the Microsoft Ecosystem - Setting up a Web presence using Internet Information Services (IIS): Web Site (HTTP, HTTPS), FTP, SMTP - Endpoint Security using a Firewall - Database Services - Messaging Services - Final Project