

**Université Saint-Joseph  
Faculté d'Ingénierie  
Institut National de la Communication et de l'Information**

**MASTER**

**SYSTÈMES ET RÉSEAUX**

**OPTION**

**SÉCURITÉ DE L'INFORMATION**

ماسٲر في الأنظمة والشبكات

فرع

حماية المعلومات

**Catalogue 2017-2018**

---

Adresse : Institut National de la Communication et de l'Information  
Campus des Sciences et Technologies  
Mkalles - Mar Roukos - Liban  
E-mail : inci@usj.edu.lb  
B.P. : 11-514 Beyrouth - Liban  
Tél. : (01) 421315 - Télécopie : (04) 532652

# **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. Admission**

### **2.1 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.

## 2.2. 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.

## 3. Compétences

<b>Compétence</b>	<b>Résultats d'Apprentissage niveau Programme (RAP)</b>
A. Concevoir un système d'information optimisé et sécurisé	A1. Identifier les besoins métier A2. Mettre en place les stratégies de gouvernance A3. Définir l'architecture intégrant toutes les composantes du système
B. Assurer l'intégration et la gestion des composantes du système d'information d'une entreprise	B1. Implémenter et configurer les composants systèmes et réseaux B2. Vérifier la conformité du système avec les besoins en termes de performances et de sécurité B3. Superviser et assurer le bon fonctionnement du système B4. Optimiser l'efficacité et le rendement du système
C. Prévenir et gérer les risques informatiques	C1. Identifier et analyser les risques qui menacent la résistance d'un système d'information C2. Définir un plan de mitigation des risques C3. Mettre en place les politiques, les procédures et les contrôles nécessaires
D. Faire preuve de qualités de management et de leadership	D1. Mettre en place et appliquer une stratégie d'entreprise D2. Gérer et diriger des équipes de travail D3. Mener des études de faisabilité D4. Identifier les enjeux et les contraintes liés à la création d'entreprises

#### **4. Programme prévisionnel**

Les matières sont réparties sur les semestres M1-1, M1-2, M2-1 et M2-2 suivant les tableaux ci-dessous (2 années d'étude).

##### **Semestre M1-1**

<b>MATIÈRE</b>	<b>Volume Horaire</b>	<b>Crédits ECTS</b>
Administration Unix	60	6
Architecture et gestion des réseaux	56	6
Gouvernance des SI	20	2
Modélisation et optimisation des réseaux	50	6
Nouvelles technologies pour réseaux IP	60	6
Windows system administration	40	4
<b>TOTAL</b>	<b>286</b>	<b>30</b>

##### **Semestre M1-2**

<b>MATIÈRE</b>	<b>Volume Horaire</b>	<b>Crédits ECTS</b>
<b>Communications unifiées</b>	<b>43</b>	<b>4</b>
Cryptographie et applications sécurisées	42	4
Gestion de projets	20	2
Projet 1		6
Réseaux sans fil	55	6
<b>Optionnelle fermées (1)</b>	<b>70</b>	<b>8</b>
<b>TOTAL</b>	<b>235</b>	<b>30</b>

(1) Matières proposées : Big data (4 crédits) ou Droit informatique (2 crédits) ou Innovation & Design Thinking (2 crédits) ou Introduction to entrepreneurship (2 crédits) ou Software defined data center (2 crédits).

##### **Semestre M2-1**

<b>MATIÈRE</b>	<b>Volume Horaire</b>	<b>Crédits ECTS</b>
Digital Forensics	20	2
Gestion des risques	20	2
Information security - standards and best practices	35	4
Information Systems Administration and Security	40	4
Piratage Ethique	35	4
Projet 2		6
Réseau d'entreprise sécurisé	35	4
Sécurité des Infrastructures Réseaux	40	4
<b>TOTAL</b>	<b>225</b>	<b>30</b>

##### **Semestre M2-2**

<b>MATIÈRE</b>	<b>Volume Horaire</b>	<b>Crédits ECTS</b>
Stage d'entreprise		30
<b>TOTAL</b>		<b>30</b>

## **5. Contenu du Programme**

### Semestre M1-1

#### **Administration UNIX - 6 crédits**

##### **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)

#### **Architecture et gestion des réseaux - 6 crédits**

##### **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.

#### **Gouvernance des SI - 2 crédits**

##### **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

## **Modélisation et optimisation des réseaux - 6 crédits**

### **Objectif**

Présentation des outils de base pour la modélisation des réseaux : processus Markoviens, files d'attente, graphes. Etude. Utilisation de ces outils pour l'étude des performances et le dimensionnement des réseaux. Introduction aux méthodes de recherche opérationnelle et leurs applications aux réseaux.

### **Contenu**

- Introduction à la notion de modélisation dans les réseaux à commutation de circuits et de paquets : performance vs. Dimensionnement.
- Introduction aux graphes comme étant un cadre global de modélisation. Graphes et recherche opérationnelle.
- Définitions et propriétés fondamentales des graphes.
- Algorithmique de base : parcours d'un graphe, composantes connexes,...
- Routage et algorithmes de plus court chemin.
- Commutation dans les réseaux locaux et l'algorithme de l'arbre couvrant.
- Flot maximal dans les réseaux de transport.
- Introduction aux phénomènes d'attentes dans les réseaux. Files d'attentes et notations
- Les files d'attentes M/M/. et les processus de naissance et de mort. Application aux commutateurs de paquets et au dimensionnement GSM.
- Les chaînes de Markov à temps discret : définition, classification des états et probabilités stationnaires. Manipulation sur Matlab sur divers exemples : processus informatiques, compagnie d'assurance, ...
- Les processus de Markov à temps continu. Probabilités stationnaires et applications diverses.
- Files d'attentes M/GI/1 multiclassées et files de priorité. Application aux réseaux multiservices et à la QoS.
- Modélisation de l'accès au médium partagé : Aloha, CSMA, .... Simulation sur Matlab.
- Introduction à la programmation linéaire et à l'optimisation : application au routage et à l'optimisation des ressources dans un réseau

à commutation de paquets.

## **Nouvelles technologies pour réseaux IP - 6 crédits**

### **Objectif**

Approfondir les protocoles de l'internet et leurs évolutions

### **Contenu**

- Rappel architecture TCP/IP et Contrôle de congestion
- Multicast (Adressage, protocoles de gestion de groupe, routage, et transport)
- Evolution IPv6 (Adressage, protocole, ICMPv6, Transitions)
- Mobilité IP (Mobile IPv4, Mobile IPv6, CellularIP)
- Commutation IP et MPLS (Concepts, fonctionnement, mise en œuvre)
- Qualité de service IP (Gestion de flux, ordonnancement, RTP/RTCP, Architectures IntServ/RSVP, DiffServ)

TD Simulation de Réseaux :

- TCP et contrôle de congestion
- Multicast et réseaux dynamiques
- RED
- MPLS

Cycle de Travaux Pratiques :

- Multicast
- IPv6
- QoS

## **Windows system administration - 4 credits (English)**

### **Objectives**

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.

### **Contents**

- 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

### Semestre M1-2

#### **Big data - 4 crédits**

##### **Objectif**

Le cours couvre différents aspects théoriques et pratiques pour la gestion des données massives.

##### **Contenu**

Calcul distribué avec MapReduce, analyse des liens dans les graphes, PageRank, recherche des ensembles similaires, recherche de motifs fréquents, identification des communautés dans les graphes, les systèmes de recommandations et de classification, Detection des ensembles séparables, Support vector machines

#### **Communications unifiées - 4 crédits**

##### **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**

#### **Cryptographie et applications sécurisées - 4 crédits**

##### **Objectif**

Initier les étudiants aux principaux thèmes de la cryptographie moderne, de la théorie aux applications.

##### **Contenu**

Introduction et présentation des risques - Concepts de base de la cryptographie - Concepts des protocoles de sécurisation : Ipsec, SSL, SET- Applications de type VPN et différentes solutions protocolaires associées - Solutions et architectures de sécurité des réseaux et des échanges - Solutions de traitement locaux : Firewall, IDS - Infrastructures de distribution des clés (PKI) - Méthodologie et politique de sécurité - Audit de réseaux.

## **Droit informatique - 2 crédits**

### **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.

## **Gestion de Projets - 2 crédits**

### **Objectif**

Le cours de « Project Management » permet aux étudiants de connaître les différentes phases d'un projet qui sont indispensables pour la bonne gestion 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

## **Innovation and design thinking - 2 credits (English)**

### **Objectives**

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.

### **Contents**

## **Introduction to entrepreneurship - 2 credits (English)**

### **Objective**

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

### **Content**

- 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

## **Projet 1 - 6 crédits**

### **Objectif**

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

### **Contenu**

## **Réseaux sans fil - 6 crédits**

### **Objectif**

Présentation des principes de base des communications sans-fil. Etude des défis et techniques de la radio large bande (broadband).  
Présentation théorique et pratique des technologies de 3ème et de 4ème génération. Etude des Réseau locaux sans-fil (WLANs) et des réseaux sans-fils hétérogènes.

### **Contenu**

- Introduction générale sur l'évolution des réseaux et standards sans-fils.
- UMTS :  
Introduction au CDMA : Equation d'interférence pour CDMA1 et WCDMA  
Services 3G et Architecture UMTS : UE, UTRAN, CN et interfaces.  
Interfaces et protocoles UTRAN, couches protocolaires.  
Canaux  
Gestion des ressources radio  
Gestion de la mobilité  
Dimensionnement et deployment
- Défis et techniques utilisées dans les communications radio large-bande
- 3.G : HSPA
- LTE : architecture et interface air.
- WLANs :  
Standard 802.11  
Architecture et déploiements  
Accès CSMA/CA  
Format des trames  
QoS
- Réseaux hétérogènes : intégration des WLANs dans les réseaux d'opérateurs pour un accès hybride.

## **Software defined data center - 2 credits (English)**

### **Objective**

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.

### **Content**

- Defining:
  - Active components of a Datacenter
  - Traditional Data center technologies
  - Cloud computing and Virtualization
    - o Concepts
    - o Different Models
    - o Technologies
    - o Security
- Virtualization technologies
  - o Systems virtualization

- Storage virtualization
- Network virtualization
  - Virtual network devices
  - SDN
- Converged Infrastructures
- Hyper-Converged Infrastructures

### Semestre M2-1

## **Digital forensics - 2 credits**

### **Objectives**

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.

The course objective is to introduce:

- 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

### **Contents**

#### **Module 1: Legal Aspects and the Need for Digital Forensics**

- Computer Forensics Overview
- Origins of Computer Forensic science
- Criminal and civil Laws
- Types of cyber and digital incidents
- Internal and external threats
- Digital Forensic challenges

#### **Module 2: First Response Model**

- Digital Evidence
- Best Practices for response
- Incidents, and Evidence Types
- Search & Seizure
- Planning and Preparation
- Evidence Handling
- Evidence Admissibility in a Court
- Documenting and Reporting Digital Evidence

### **Module 3: Computer & Mobile Forensics**

- Understanding Hard Disks and File Systems
- Searching and Seizing Devices
- Windows/Linux Workstations Forensics
- Smartphones Forensics
- Steganography and Image File Forensics

### **Module 4: Information Systems Forensics**

- Tracking Emails and Investigating Email Crimes
- Investigating network attacks
  - LAN / WAN
  - Wireless
- Investigating Web Attacks
- Password Crackers
- Investigating E-Frauds

### **Module 5: Using SIEM for Security Forensics**

- Event sources
- Audit Trails & Log Management
- Log Capturing and Correlation
- Detection rules
- Big Data for security events

## **Gestion des risques - 2 crédits**

### **Objectif**

Le concept de gestion des risques a fait son apparition à la fin des années 50 aux États-Unis dans le domaine financier, en relation avec des questions d'assurance. Par la suite, la notion de gestion des risques a été étendue à d'autres domaines, notamment l'environnement, la gestion de projet, le marketing, ainsi que la sécurité informatique.

La gestion des risques est définie par l'ISO comme l'ensemble des activités coordonnées visant à diriger et piloter un organisme vis-à-vis du risque. On dégage en général trois finalités à la gestion des risques pour les systèmes d'information :

1. Améliorer la sécurisation des systèmes d'information.
2. Justifier le budget alloué à la sécurisation du système d'information.
3. Prouver la crédibilité du système d'information à l'aide des analyses effectuées.

Afin de mieux appréhender la gestion des risques, ce cours a pour but de présenter l'ensemble des concepts du domaine, ainsi que les méthodes actuellement utilisées.

### **Contenu**

- L'identification des risques
- L'analyse des risques
- La réduction des risques
- Le contrôle des risques

## **Information security - standards and best practices - 4 credits**

### **Objectives**

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.

### **Contents**

#### *A- Introduction:*

- Information Security
- The Need for Information Security
- How to define security needs
- Risk assessment
- Selection of controls
- The starting point for information security

#### *B- Security policy:*

- The implementation of a security policy
- The content of a security policy
- The review and audit of the policy

#### *C- Organization of information security*

- Internal organization
  - Management commitment to information security
  - Information security co-ordination
  - Allocation of information security responsibilities
  - Authorization process for information processing facilities
  - Confidentiality agreements
  - Contact with authorities and other interest groups
  - Independent review of information security
- External parties
  - Identification of risks related to external parties
  - Addressing security when dealing with customers
  - Addressing security in third party agreements

#### *D- Asset management*

- Inventory of assets
- Custody and ownership definition
- The role of information security
- Data and information classification

- E- *Human resources Security*
  - Prior to employment
  - During employment
  - Change or termination of employment
- F- *Physical and Environmental Security*
  - Scope definition
  - Implementation of security control
  - Equipment security
- G- *Communication and operations management*
  - Procedures and defining responsibilities
  - Exchange of information
  - Capacity planning
  - Network security
  - Media Safety
  - Saving data
  - E-commerce
  - Monitoring and detection controls (Audit logs)
- H- *Access Control*
  - Users responsibilities
  - Managing user access
  - Operating systems access control
  - Application and information access control
  - Network access control
  - User mobility and access control
- I- *Information Security incident Management*
  - Management methodology
  - Procedures
- J- *Business Continuity Management*
  - Methodology and life Cycle of a Business Continuity Management
  - Business Continuity Plan

## **Information systems administration and security - 4 credits (English)**

### **Objectives**

Learn the basic techniques of information security and administration.

### **Contents**

Basic mechanisms: identification, authentication, access control, process protection, securing file systems and workstations - Security administration - Database administration and security - Information protection: redundancy (RAID technologies, backup, ...), replication, disaster recovery and business continuity planning (BCDR), encryption, access rights.

Lab sessions: Implementation and administration of database security - Implementation and administration of storage security.

## **Piratage Ethique - 4 crédits**

### **Objectif**

Comprendre et détecter les attaques sur un SI - Définir l'impact et la

portée d'une vulnérabilité - Réaliser un test de pénétration - Corriger les vulnérabilités - Sécuriser un réseau et intégrer les outils de sécurité adéquats.

### **Contenu**

Principes de sécurité - Les attaques - Attaques sur les équipements - Attaques sur les réseaux - Attaques logiques - Attaques sur les systèmes - Attaques sur les services - Protection et contre-attaque - Quelques scénarios d'intrusion.

## **Projet 2 - 6 crédits**

### **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 ...

## **Réseau d'entreprise sécurisé - 4 crédits**

### **Objectif**

Maîtriser 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.

## **Sécurité des infrastructures réseaux - 4 crédits**

### **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.

### Semestre M2-2

#### **Stage d'entreprise - 30 crédits**

##### **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.