EURECOM
Sophia Antipolis

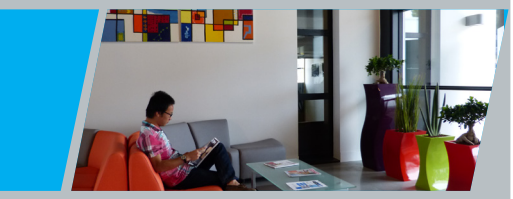
EURECOM une grande école d'ingénieurs
au coeur de la société numérique

Cti
Commission
des Titres d'Ingénieur

Ingénieur de spécialisation

Diplôme accrédité par la Commission des Titres d'Ingénieur, CTI, Bac+6

Sécurité des Systèmes Informatiques et des Communications



liste des cours 2016-2017

Cette formation offre les connaissances techniques nécessaires aux ingénieurs chargés de concevoir des systèmes sécurisés et aux administrateurs systèmes chargés d'assurer la sécurité informatique et réseau au sein d'une entreprise.

L'accent est mis sur l'analyse des vulnérabilités, la conception et la gestion des mécanismes de sécurité dans le domaine des réseaux fixes et mobiles, des systèmes informatiques et du traitement d'image.

Tous les cours sont dispensés en anglais

Diplôme ouvert à la formation continue

Institut Mines-Télécom

Ecole de
l'Institut Mines Telecom

PLAN

I. **INTRODUCTION** **2**
OBJECTIFS 2
MODALITES 2

II. COMPETENCES VISEES ET EMPLOIS TYPES **3**
COMPÉTENCES VISÉES 3
SECTEURS D'ACTIVITÉ 3
EMPLOIS TYPE 3

III. LISTE DES COURS PROPOSÉS AU SEIN DE LA FORMATION **4**

IV . ORGANISATION DU CURSUS **5**

DESCRIPTION DES COURS **5**

COURS TECHNIQUES **6**
ANALYSE STATISTIQUE DE DONNÉES 6
APPLICATIONS DE SÉCURITÉ DANS LES RÉSEAUX ET SYSTÈMES DISTRIBUÉS 6
CYBERCRIMINALITÉ ET FORENSIQUE INFORMATIQUE 7
INTRODUCTION AUX RÉSEAUX ET À INTERNET 7
RÉSEAU MOBILE 8
SÉCURITÉ DES COMMUNICATIONS 9
SÉCURITÉ DES SYSTÈMES ET RÉSEAUX 9
SYSTÈMES DE COMMUNICATIONS MOBILES 11
SYSTÈMES DISTRIBUÉS ET CLOUD COMPUTING 12
THÉORIE DES JEUX 12
TRAITEMENT D'IMAGES EN SÉCURITÉ: TATOUAGE ET BIOMÉTRIE 13
TRAITEMENT ET COMPRESSION D'IMAGES FIXES ET ANIMÉES 13

COURS NON TECHNIQUES **14**
APPROCHES SOCIOLOGIQUES DES TECHNOLOGIES DES TÉLÉCOMMUNICATIONS 14
DÉVELOPPEMENT PERSONNEL ET TEAM LEADERSHIP 14
ENTREPRENARIAT ET CAPITAL-RISQUE 15
GESTION DE PROJET 15
INTRODUCTION AU MANAGEMENT 16
INTRODUCTION GÉNÉRALE AU DROIT : LES CONTRATS ET LA CRÉATION DE SOCIÉTÉ 17
PROPRIÉTÉ INTELLECTUELLE 17
SIMULATION D'ENTREPRISE 18

CONTACTS **19**

I. INTRODUCTION

Depuis la fin des années 90, l'informatique et les systèmes de communication font partie intégrante de la vie privée et professionnelle de la majorité des occupants de notre planète.

En plus des avancées en cryptographie comme la mise en œuvre à grande échelle de la signature numérique et des moyens de chiffrement grand public, les deux dernières décennies ont aussi vu naître des domaines tout à fait nouveaux comme la sécurité des réseaux et les transactions sécurisées avec Internet, la sécurité des communications mobiles et sans fil avec les développements des nouvelles technologies de communication, sans oublier la protection et la gestion des droits pour les contenus multimédias.

Dans ce contexte, tout acteur des moyens informatiques et des communications, du simple utilisateur à l'expert technique, doit prendre en compte la malveillance et se prémunir contre ses effets en ayant recours aux techniques de sécurité. La connaissance des vulnérabilités et des solutions techniques pour la protection devient aussi indispensable pour les ingénieurs qui utilisent ou créent des systèmes informatiques et des systèmes de communication.

Une formation technique en sécurité doit donc se situer comme un prolongement de tous ces domaines qui forment le socle des compétences acquises et couvrir les sujets aussi variés que la cryptographie, la détection et l'analyse des logiciels malveillants, les logiciels et systèmes informatiques sécurisés, la sécurité des réseaux fixes, des réseaux mobiles et du sans fil, la stéganographie, les techniques biométriques et les méthodes de protection de la vie privée.

OBJECTIFS

Cette formation a le but d'offrir les connaissances techniques nécessaires aux ingénieurs chargés de concevoir des systèmes sécurisés et aux administrateurs système chargés d'assurer la sécurité informatique et réseau au sein d'une entreprise ou d'un organisme public. L'accent est mis sur l'analyse des vulnérabilités, la conception et la gestion des mécanismes de sécurité dans le domaine des réseaux fixes et mobiles, des systèmes informatiques et du traitement d'image. Les techniques de sécurité étudiées comprennent la cryptographie et ses applications, la détection et l'analyse des logiciels malveillants, les mécanismes de sécurité dédiés à la protection des communications, des réseaux et des applications informatiques distribuées, la protection des images et les techniques biométriques.

MODALITES

Le diplôme d'ingénieur de spécialisation est un titre reconnu par la CTI de niveau Bac + 6 et inscrit au RNCP (Niveau I).
La formation est ouverte à la **Formation Initiale et Continue.** Elle s'adresse donc aussi bien à des étudiants en poursuite d'études qu'à des ingénieurs et chercheurs en poste.

II. COMPETENCES VISEES ET EMPLOIS TYPES

COMPÉTENCES VISÉES

- Définir l'architecture d'un système de communication sécurisé
- Concevoir les composantes d'un système de communication sécurisé
- Concevoir des composantes logicielles résistant aux attaques informatiques
- Concevoir les mécanismes de sécurité destinés à un système informatique
- Réaliser un prototype logiciel pour un système informatique sécurisé
- Réaliser les modules logiciels pour des fonctions spécifiques de sécurité
- Concevoir de nouveaux algorithmes pour la sécurité des systèmes informatiques
- Évaluer les performances de solutions de sécurité existantes
- Mettre en œuvre le plan directeur d'un réseau sécurisé
- Mettre en œuvre le plan directeur d'un système d'information sécurisé
- Mener une campagne d'audit de sécurité pour un réseau d'entreprise ou un système d'information
- Effectuer des tests de vulnérabilité d'applications logicielles distribuées
- Assurer la gestion de la sécurité informatique au sein d'une entreprise
- Participer à la conception de mécanismes de sécurité pour les nouvelles applications informatiques ou les nouvelles technologies de communication
- Participer aux travaux de normalisation dans le domaine de la sécurité informatique et réseaux
- Siéger dans des instances qui régissent la protection de la vie privée dans les systèmes informatiques et les réseaux (cnil, wwwc, . . .)
- Effectuer l'étude de marché dans le domaine des services de sécurité

SECTEURS D'ACTIVITÉ

- Centre de R&D
- Industriels fournisseurs de technologies pour les systèmes de communications
- Opérateurs de Systèmes de Communication
- Opérateurs Mobiles
- Organismes de standardisation dans le domaine de la sécurité
- Secteur tertiaire mettant en œuvre des transactions sécurisées (banques, assurances, …)
- Sociétés de Conseil en Sécurité, Informatique et Réseau

EMPLOIS TYPE

- Architecte de solutions en sécurité
- Chef de produit
- Chef de projet
- Consultant en organisation de la sécurité des systèmes informatiques
- Ingénieur R&D, intégration
- Ingénieur technico-commercial
- Responsable sécurité des systèmes informatiques d'une entreprise

III. LISTE DES COURS PROPOSÉS AU SEIN DE LA FORMATION

(voir Chapitre IV sur l'organisation académique et le nombre de cours minimum à valider)

SEMESTRE AUTOMNE		Durée (h/semestre)	ECTS
Unités d'Enseignement Techniques			
	Analyse statistique de données	21	3
	Codage d'Images	21	3
	Introduction aux Réseaux et à Internet	42	5
	Sécurité des Communications	42	5
	Sécurité Système & Réseaux	42	5
	Systèmes distribués – Cloud Computing	42	5
	Systèmes de Communications Mobiles	42	5
	Théorie des Jeux	21	3
	Traitement d'Images Numériques	42	5
Unités d'Enseignement non techniques			
	Développement Personnel et Team Leadership	42	5
	Développement durable des TIC	21	3
	Entreprenariat et capital risque	21	3
	Innovation et développement de produits	21	3
	Introduction au Management	42	5
	Droit de la propriété Intellectuelle	21	3
Cours de langue			
	Anglais	22	1
Projet			
	90 heures	90	7

SEMESTRE Printemps		Durée (h/semestre)	ECTS
Unités d'Enseignement Techniques			
	Applications de sécurité dans les réseaux et systèmes distribués	21	3
	Cybercriminalité et Forensique Informatique	42	5
	Réseau Mobile	21	3
	Réseaux Mobiles Avancés	21	3
	Sécurité matérielle	21	3
	Spécification et Vérification formelles des systèmes	21	3
	Traitement d'images en sécurité : tatouage et biométrie	21	3
Unités d'Enseignement non techniques			
	Simulation d'entreprise	42	5
	Introduction Générale au Droit	21	3
	Gestion de projet	42	5
	Approches sociologiques des TIC	21	3
Cours de langue			
	Anglais	21	1
Projet			
	90 heures	90	7

IV . ORGANISATION DU CURSUS

Le cursus du diplôme d'ingénieur de spécialisation s'étend **sur 16 mois** (deux semestres académiques et un stage de 22 semaines minimum en entreprise). Le cursus s'appuie sur des cours magistraux, des travaux dirigés en laboratoires et des projets d'application pratique (études de cas, challenges hacking en ligne…).

Le cursus est équilibré entre cours théoriques et cours appliqués afin de permettre aux candidats d'être rapidement opérationnels à l'issue de la formation. Des cours non techniques (droit, gestion de projet, création d'entreprise...) enseignés par des professeurs d'écoles de commerce et experts industriels, complètent le cursus afin d'apporter une double compétence.

EURECOM entretient des liens très forts avec des entreprises impliquées dans la sécurité informatique. Le centre de recherche européen de l'entreprise américaine *SYMANTEC* se trouve au même sein des locaux d'EURECOM. Des experts d'entreprises interviennent régulièrement dans les cours (ANSSI, GOOGLE...)

UNE APPROCHE PÉDAGOGIQUE TRÈS PROFESSIONALISANTE

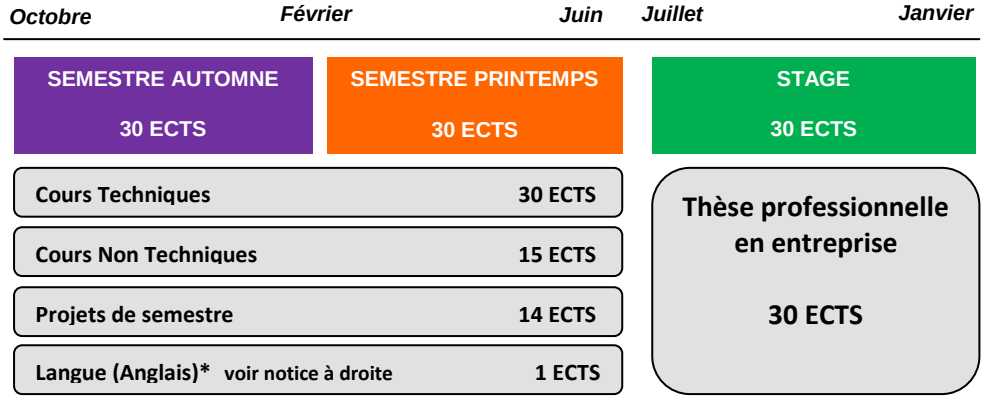
Le cursus du diplôme d'ingénieur de spécialisation vise l'acquisition et la maitrise de compétences clés permettant aux diplômés d'atteindre rapidement le niveau requis par les entreprises. Une place essentielle est accordée aux travaux d'application pratique via les projets de semestre et le stage professionnel.

PROJET DE SEMESTRE:
Chaque semestre, les étudiants choisissent un sujet de projet parmi une liste de choix proposés. Les projets s'appuient sur des problématiques actuelles en sécurité informatique. Encadrés par les professeurs, les étudiants doivent développer des solutions ou résoudre des difficultés identifiées. Les sujets sont souvent proposés par les partenaires industriels d'EURECOM.

STAGE EN ENTREPRISE:
Le dernier semestre est un stage de 6 mois qui se déroule dans une entreprise. L'étudiant met en application les concepts appris en cours tout en travaillant sur une thèse professionnelle autour d'un thème d'intérêt industriel en sécurité informatique.
EURECOM met à disposition des étudiants une importante base de stages en France et à l'étranger.

Un nombre total de **90 crédits (ECTS)** doit être atteint pour obtenir le diplôme d'ingénieur de spécialisation. Chaque type de cours est équivalent à un certain nombre de crédits et équivaut à 3h d'enseignement par semaine. Les étudiants doivent ainsi effectuer un choix parmi les cours proposés pour obtenir le nombre de crédits requis durant les deux semestres académiques.

CALENDRIER ACADEMIQUE



* **Crédit de langue anglaise** :
Ce crédit est automatiquement validé si l'étudiant fournit un test récent de connaissance en anglais (TOEIC, TOEFL…) attestant d'un niveau B2 minimum. Le test doit dater de moins de trois ans. Sinon le candidat devra passer un test de langue pour attester de son niveau avant la fin de la formation.

DESCRIPTION DES COURS

COURS TECHNIQUES

ANALYSE STATISTIQUE DE DONNÉES (Semestre Automne)

Patrick LOISEAU

L'objectif du cours est de donner aux étudiants des méthodes statistiques simples et efficaces pour analyser des données. Ces méthodes sont d'une importance cruciale dans de nombreuses situations car elles permettent de répondre à des questions telles que :
'Est-ce que cette amélioration de performance est significative ?', 'Quelle est l'incertitude sur ce résultat ?', 'Comment puis-je prédire le résultat d'une nouvelle observation de mon système à partir de mesures passées ?', 'Quels facteurs ont un impact significatif sur la performance de mon système ?', et beaucoup d'autres.

L'analyse mathématique des méthodes sera brièvement abordée, mais le cours se concentrera principalement sur la compréhension des méthodes et des situations dans lesquelles elles peuvent être appliquées (quelle méthode appliquer, qu'en attendre, etc.).
Le cours présentera des méthodes génériques pouvant s'appliquer sur des données provenant de n'importe quelle application, et non pas un domaine d'application spécifique. Des exemples seront donnés dans différents domaines (réseaux, ingénierie, etc.).
Le cours traitera les sujets suivants :

- Bases de probabilités : rappel de toutes les notions de probabilités nécessaires à la suite du cours (variables aléatoires, distributions, principales inégalités et théorèmes limites (loi des grands nombres, théorème de la limite centrale))
- Intervalles de confiance : synthèse des données, principales méthodes pour le calcul d'intervalles de confiance (grands échantillons, cas normal), bootstrap
- Modèles et ajustement : estimation de paramètres, maximum de vraisemblance, méthode des moindres carrés, régression linéaire, ajustement de distributions
- Tests statistiques : cadre de Neyman-Pearson et principes fondamentaux des tests d'hypothèses, tests simples, bootstrap, analyse de la variance

APPLICATIONS DE SÉCURITÉ DANS LES RÉSEAUX ET SYSTÈMES DISTRIBUÉS (Semestre Printemps)

Refik MOLVA

Ce cours présente les principales applications des mécanismes de sécurité dans le cadre des réseaux et des systèmes distribués. Le cours traite des approches de filtrage réseau basées sur les pare-feu, des suites de protocoles normalisés conçus pour la protection des échanges de données et le contrôle réseau sur l'Internet, les protocoles de sécurité pour les réseaux sans fil et des solutions pour les réseaux cellulaires et mobiles. Les thèmes suivants sont abordés dans ce cours :

- Contrôle d'Accès : Modèles de contrôle d'accès, contrôle d'accès à base de rôle, certificats d'attributs, SPKI, XACML
- Contrôle d'Accès Réseau et les Pare-Feu : Filtrage de paquets, passerelles applicatives, passerelles de circuits, conversion des adresses (NAT), configurations de pare-feu
- Sécurité Cryptographique pour l'Internet : Protocoles IPsec, Oakley/ISAKMP, TLS/SSL, VPN/SSL, sécurité cryptographique dans le DNS, le routage et SMTP
- Sécurité dans les Réseaux Mobiles : EAP, Radius, Diameter, sécurité dans les réseaux sans fil, mécanismes de sécurité dans GSM, 3GPP, DECT et dans l'IP Mobile.

CYBERCRIMINALITÉ ET FORENSIQUE INFORMATIQUE (Semestre Printemps)

Davide BALZAROTTI

Le cours Cybercriminalité et Forensique Informatique est la suite du cours Sécurité Système et Réseau. L'idée est de présenter différentes approches pour analyser et détecter les logiciels malveillants et faire face aux machines compromises. Ce module comptant un certain nombre d'exercices de programmation, il est fortement recommandé aux étudiants intéressés d'avoir de l'expérience en la matière.

Ce cours présente les techniques existantes pour combattre la cybercriminalité en se basant sur les connaissances acquises pendant le cours "***Sécurité Système et Réseau***". Il s'agira principalement d'étudier les différentes approches mises en oeuvre par les experts en sécurité informatiques afin d'analyser les attaques informatiques à grande échelle et de les prévenir.

INTRODUCTION AUX RÉSEAUX ET À INTERNET (Semestre Automne)

Yves ROUDIER

Adlen KSENTINI

Ce cours offre un aperçu général des réseaux informatiques en traitant des niveaux d'applications, des transports, des réseaux et liaison.

Il introduit les concepts de base des réseaux ainsi que quelques protocoles utilisés dans l'Internet à travers les sujets suivants :

- Aperçu des réseaux informatiques : Packet switching, concepts de retard et de pertes, médium physique, protocoles en couche, structures peer-to-peer sur Internet.
- Niveau application : Web, E-mail, DNS, introduction à la programmation de sockets.
- Niveau transport : Principes de transport fiable, UDP et TCP, principes du contrôle de congestion.
- Niveau réseau et routage : Théorie du routage par l'état des liaisons et par vecteurs de distance, routage hiérarchique : adressage IPv4, CIDR, RIP
- Niveau liaison : Détection d'erreur et techniques de correction d'erreur, protocoles d'accès multiples, adressage LAN, ARP, Ethernet.

RÉSEAU MOBILE (Semestre Printemps)

Christian BONNET

Ce module traite de la mobilité dans les réseaux IP (Internet ou réseaux privés). En particulier, on détaillera les différents mécanismes permettant la mobilité dans les réseaux basés sur IPv6. Les thèmes suivants sont abordés dans ce cours :

- Mécanismes de mobilité dans les réseaux IPv4
- Comparaisons des différentes propositions historiques
- Mécanismes de base IPv6
- Mobile IPv6
- Mobilité Hiérarchique (HMIP)
- Mécanismes de Handover basés sur IPv6
- Mobilité globale v.s. mobilité locale
- NetLMM et proxyMIP
- Mobilité de sous réseaux (NEMO)
- Les schémas de mobilité au-dessus de la couche réseau

RESEAUX MOBILES AVANCES (Semestre Printemps)

Navid NIKAEIN

Ce cours s'adresse aux étudiants désirant apprendre les nouveaux standards et technologies émergentes et avancés utilisés dans les réseaux futur sans fil cellulaires, maillés, et ad-hoc ainsi que les réseaux de capteurs et d'actionneurs sans fil.

Il couvre essentiellement les applications potentielles et les couches réseau et transport en donnant pour chacune les protocoles et techniques proposés et les travaux de standardisation et de recherche en cours.

DESCRIPTION

- Le contenu de ce cours est le suivant :
  Les réseaux sans fil WiMAX (802.16) : introduction, applications et architectures, la gestion de la qualité de service, la gestion de la mobilité dans 802.16e, etc.
- Les réseaux de capteurs sans fils: introductions applications et architectures, les méthodes d'auto-organisation, les protocoles de transport fiable, etc.
- Les réseaux maillés sans fils: introduction, applications et architectures, les protocoles de routage, mécanismes d'équilibrage de charge et de la QoS, techniques d'allocation dynamique de canaux, etc.
- Les réseaux véhiculaires sans fil : introduction, applications et architectures, protocoles de broadcast, solutions Delay-Tolernent Networks pour les communications inter-véhicules et entre les véhicules et l'infrastructure.

-

SÉCURITÉ DES COMMUNICATIONS (Semestre Automne)

Refik MOLVA

Ce cours est une introduction à la cryptographie et aux mécanismes de communication sécurisée qui sont basés sur la cryptographie. Ce cours traite aussi bien des aspects fondamentaux tels que les primitives mathématiques sous-jacentes à la cryptographie que des aspects appliqués comme la conception des principaux algorithmes de chiffrement et de hachage et la mise en œuvre de la signature numérique, l'authentification et la gestion des clés. Les thèmes suivants sont abordés dans ce cours :

- **Cryptographie** : Historique des algorithmes de chiffrement, évaluation de la sécurité, entropie, fonction d'équivocation des clés, distance d'unicité, sécurité parfaite, one-time pad
- **Algorithmes de Chiffrement** : Algorithmes symétriques, modèle de Feistel, DES, théorie des nombres, IDEA, AES, mise en cascade des chiffres, chiffrement par flots, RC4, algorithmes asymétriques, fonction à sens unique, Diffie-Hellman, RSA, El Gamal, cryptographie sur les courbes elliptiques
- **Mécanismes de Chiffrement et d'Intégrité des Données** : Attaques statistiques, modes de chiffrement (CBC, CFB, OFB, CTR), fonctions de hachage et intégrité des données, MAC et MDC, propriétés de sécurité spécifiques, solutions alternatives pour la mise en œuvre du MAC
- **Signature Numérique et Non-Répudiation** : Algorithme de signature El Gamal, norme de signature numérique, mécanismes de non-répudiation
- **Authentification et Gestion des Clés** : Protocoles d'authentification, mots de passe, dispositifs personnels, gestion des clés, distribution des clés symétriques, Kerberos, certification des clés publiques et les infrastructures de certification, contrôle d'usage des clés

SÉCURITÉ DES SYSTÈMES ET RÉSEAUX (Semestre Automne)

Aurélien FRANCILLON

Ce cours introduisant les concepts de sécurité à travers l'étude des vulnérabilités existant dans les systèmes informatiques, les réseaux d'ordinateurs et les applications web. C'est un cours à caractère expérimental où les étudiants seront amenés à mettre en œuvre des attaques et développer des contremesures pratiques.

Ce cours a pour but de sensibiliser les étudiants aux problèmes de sécurité communément rencontrés sur les systèmes réels. Un des buts de ce cours est d'apprendre aux étudiants à penser comme un attaquant, cela les aidera par la suite à la conception de systèmes sécurisés et à éviter les erreurs classiques.

Une expérience en programmation de base (C) et une connaissance des concepts de base en réseaux et systèmes d'exploitation est recommandé.

Les thèmes suivants sont abordés dans ce cours :

- Sécurité de Windows et Unix
- Race Conditions
- Corruption Mémoire, Exploitation et Contre-mesures Modernes

- Trusted Computing
- Sécurité Web
- Sécurité des réseaux sans fils
- Sécurité Réseaux
- Le Test en Sécurité
- Security des Smartphones
- Introduction au Malware

SECURITE MATERIELLE (Semestre Printemps)

Renaud PACALET

Les applications embarquées qui ont un besoin fort de sécurité utilisent des algorithmes et des protocoles cryptographiques élaborés, réputés robustes face aux attaques logiques. Ces algorithmes et protocoles sont implémentés sous forme logicielle ou matérielle au sein du système. Malheureusement pour les concepteurs de systèmes sécurisés tout calcul doit être exécuté par un dispositif matériel, microprocesseur ou opérateur dédié, et tout dispositif matériel laisse transparaitre des traces mesurables de son activité (consommation électrique, rayonnements, temps de calcul, etc.) qui peuvent être mis à profit par un attaquant pour extraire des secrets enfouis. Le même attaquant peut également perturber le fonctionnement du système en modulant sa tension d'alimentation, sa température de fonctionnement, sa fréquence d'horloge, en le bombardant avec un laser, voire même en le modifiant. D'autres classes d'attaques visent les bus de communication sur les cartes électroniques et ont déjà été utilisées avec succès pour contourner les protections de consoles de jeu et d'autres équipements grand public.
Ce module présente un panorama de différentes attaques connues. Pour chacune d'entre elles on mettra en évidence les hypothèses fondamentales de leur mise en œuvre et on présentera les possibles contre-mesures.

L'objectif est d'informer les étudiants sur l'existence de ces menaces, de leur donner des pistes
concernant les possibles contre-mesures et de les préparer ainsi à concevoir des dispositifs plus sûrs. Les cours sont complétés par deux séances de travaux pratiques dédiées aux attaques en temps de calcul et en consommation électrique. Pendant ces séances les étudiants découvriront l'impressionnante efficacité pratique de ces attaques et tenteront de protéger la cible à l'aide de contre-mesures.

SPECIFICATION ET VERIFICATION FORMELLES DES SYSTEMES (Semestre Printemps)

Rabea AMEUR

Ce cours vise à donner aux étudiants les notions de base de la spécification et la vérification formelles. L'accent est particulièrement mis dans cet enseignement sur l'utilisation pratique des concepts rencontrés.

OBJECTIFS :

- Le développement de systèmes critiques, tels que les systèmes dont les défaillances peuvent avoir des conséquences catastrophiques, nécessite l'utilisation de méthodes de conception fiables basées sur des approches formelles. Les méthodes formelles sont des méthodes rigoureuses, basées sur la théorie. Elles permettent donc de raisonner sur les systèmes et de les analyser afin de démontrer leur validité par rapport à certaines propriétés données. L'utilisation de ces méthodes est souvent associée au savoir-faire et aux compétences des développeurs dans le domaine.
- Ce cours vise à donner aux étudiants les notions de base de la spécification et la vérification formelles.
- L'accent est particulièrement mis dans cet enseignement sur l'utilisation pratique des concepts rencontrés.

CONTENU :

- Les techniques de spécification et vérification formelles de systèmes.
- Un exemple de méthodologie formelle, la méthode B.

SYSTÈMES DE COMMUNICATIONS MOBILES (Semestre Automne)

Christian BONNET

Le but de ce cours est de présenter une série de systèmes de communications mobiles afin de synthétiser les connaissances acquises dans des cours fondamentaux. Ce cours permet d'explorer les standards existants et émergeants et de comprendre l'évolution des différents services mobiles. Chaque type de système est présenté dans son contexte d'utilisation. Le module s'intéresse principalement à montrer la convergence entre les réseaux mobiles et les réseaux fixes. Les systèmes abordés sont les suivants :

Système 2G : GSM

- Approche Circuit : procédures globales de gestion de la Mobilité et d'appels circuit mobiles
- Architecture de l'interface radio (canaux logiques, piles protocolaires)
- Architecture du cœur de réseau

Systèmes 2.5 G : GPRS/EDGE

- Impact du "Packet Switching" : Procédures du "Core Network" et sur l'interface radio

Systèmes 3G et au-delà: UMTS, HSDPA

- Impact des nouvelles technologies de transmission (WCDMA, Packet Scheduling)
- Introduction au 3GPP LTE (Long Term Evolution)

SYSTÈMES DISTRIBUÉS ET CLOUD COMPUTING (Semestre Automne)

Pietro MICHIARDI

Le but de ce cours est de fournir une vue d'ensemble sur les sujets et les tendances récentes des systèmes distribués et le Cloud Computing. Nous discuterons des techniques logiciel utilisées pour la construction et la programmation des systèmes fiables et scalable.
Nous aborderons également la conception d'architecture des centres de données modernes et les techniques de virtualisation qui constituent un thème central du paradigme de «Cloud computing». Le cours est complété par un certain nombre de séances de laboratoire pour obtenir une expérience pratique avec **Hadoop** et la conception des algorithmes scalable, avec **MapReduce**.

Compétences visées:

- Comprendre, identifier et utiliser les architectures de systèmes distribués
- Conception et implémentation d'algorithmes distribués pouvant passer a l'échelle
- Comprendre et utiliser les systèmes de stockage distribués

THÉORIE DES JEUX (Semestre Automne)

Patrick LOISEAU

Ce cours est une introduction à la théorie des jeux. La théorie des jeux étudie les interactions entre "agents" dont les objectifs dépendent des actions des autres et non seulement des leurs. Elle permet de modéliser et de comprendre de nombreux interactions stratégiques dans le monde réel, par exemple en économie.
Ce cours introduit les principaux concepts de la théorie des jeux (équilibre de Nash, etc.) et les illustrent à partir d'exemples tirés de l'économie, des sciences politiques, de l'informatique, de l'ingénierie, etc.
Le but de ce cours est de présenter les fondements de la théorie des jeux avec un niveau de détail suffisant pour que les étudiants puissent : sentir l'importance de la théorie des jeux dans la compréhension des interaction dans le monde réel et appliquer la théorie des jeux dans les propres applications.

Le cours traitera les sujets suivants :
- Jeux sous forme normale, dominance, meilleure réponse, équilibre de Nash
- Stratégies mixtes et équilibre de Nash, théorèmes d'existence, calcul
- Théorie évolutive, équilibre corrélé, stratégies minimax
- Jeux séquentiels, forme extensive, induction, équilibre parfait
- Jeux répétés, jeux stochastiques
- Jeux à information incomplète, équilibre Bayésien

TRAITEMENT D'IMAGES EN SÉCURITÉ: TATOUAGE ET BIOMÉTRIE (Semestre de Printemps)

Jean-Luc DUGELAY

Tatouage : Le tatouage permet aux propriétaires ou fournisseurs de contenus de cacher de manière invisible et robuste un message dans un document multimédia numérique, avec pour principal objectif de défendre les droits d'auteurs ou l'intégrité. Il existe un compromis délicat entre plusieurs paramètres : capacité, visibilité et robustesse.

Biométrie : La sécurité utilise trois types d'authentification : quelque chose que vous connaissez, quelque chose que vous possédez ou quelque chose que vous êtes : une biométrie. Parmi les biométries physiques, on trouve les empreintes digitales,la géométrie de la main, la rétine, l'iris ou le visage. Parmi les biométries comportementales, on trouve la signature et la voix. Chaque biométrie inclut des avantages et inconvénients, en termes de performances, coûts, acceptation de la part des utilisateurs etc. Les systèmes actuels s'orientent donc vers des solutions multimodales. Dans un futur proche, la biométrie devrait jouer un rôle essentiel en sécurité, pour le commerce électronique, mais aussi pour la personnalisation.

Dans ce cours, il sera plus particulièrement étudié les techniques d'identification et vérification des personnes à partir de signaux image et vidéo (acquisition, traitements et algorithmes, performances).

TRAITEMENT ET COMPRESSION D'IMAGES FIXES ET ANIMÉES (Semestre d'Automne)

Jean-Luc DUGELAY

Ce cours couvre les techniques de base en traitement d'images fixes et animées et dresse un panorama des méthodes actuelles en codage de source.

Les points suivants seront traités :

- Outils de base en traitement d'images : Filtrage, histogramme, détection de contours et segmentation, estimation de mouvement, transformée de Hough, morphologie mathématique, couleurs
- Compression : Le codage de source est un élément clé de tout système de communication. En effet, les données multimédia (en particulier image et vidéo) nécessitent des techniques de compression efficaces afin de les transmettre ou de les stocker.
- Images fixes : Fax et JBIG : Huffman, codage par plages GIF et JPEG : LZW, MICDA, DCT, SQ
- Vidéo H.26x : appariements de blocs MPEG-x (1,2 et 4)
- Techniques émergentes : Quantification vectorielle (DVI) Introduction au codage fractal Introduction aux codages sous-bandes et ondelettes (JPEG 2000) Implantations, applications et utilisations des systèmes de compression Introduction aux traitements dans les domaines compressés.

COURS NON TECHNIQUES

APPROCHES SOCIOLOGIQUES DES TECHNOLOGIES DES TÉLÉCOMMUNICATIONS

On a souvent tendance à opposer le Technique au Social, et à les concevoir comme des entités autonomes et distinctes. Pourtant cette scission est remise en cause par la sociologie : elle a montré que le succès/échec des innovations techniques repose sur les caractéristiques des organisations et des interactions dans lesquelles ces innovations s'inscrivent. Cet enseignement vise à initier les étudiants à une sociologie des TIC. L'objectif est de favoriser leur compréhension des problèmes d'usage et de résistances qu'ils pourront rencontrer lorsqu'ils seront amenés à concevoir des produits nouveaux ou à penser des changements en entreprise. Le cours s'appuiera sur des études de cas portant aussi bien sur les usages grand public et professionnels de technologies de l'information et de la communication, que sur l'introduction d'innovations en entreprise, ou sur des expérimentations de prototypes. Des méthodes variées seront présentées pour initier les étudiants aux démarches d'enquête sociologique.

Approche des interactions distantes : Chaque dispositif d'interaction distante se base, explicitement ou implicitement, sur un modèle de l'interaction interpersonnelle et du contexte d'usage.

- Communications mobiles : conversations écrites et vocales depuis des téléphones mobiles. Etudes de cas basées sur des enregistrements audio et des captures d'écran.
- Vidéocommunication, téléprésence. Présentation et discussion d'études conduites sur les usages de différents systèmes visiophoniques, en contexte professionnel ou domestique.

Approche de l'innovation

La technique c'est beaucoup de gens, beaucoup d'objets, beaucoup de symboles; mais c'est aussi des organisations, des habitudes, des valeurs. Toute innovation peut être comprise non seulement à partir de ses vertus intrinsèques mais aussi à partir des processus dont elle découle.

- L'entreprise comme un système socio-technique
- Réseaux sociaux et logiques d'action
- Les conditions de production de l'innovation: coopération et consensus
- Une grille d'analyse pour aborder l'innovation

Initiation aux méthodes d'enquête de la sociologie des TIC Observer les activités

- Enregistrements audio et vidéo Questionner les individus et les groupes
- Entretiens et Focus Group

DÉVELOPPEMENT PERSONNEL ET TEAM LEADERSHIP

L'objectif global du programme est de permettre à l'étudiant de réaliser leur potentiel et à augmenter les performances d'eux-mêmes et de leurs membres de l'équipe, maintenant et dans l'avenir. Les objectifs sont à gagner la sensibilisation essentielle et les compétences nécessaires pour assumer ses responsabilités en tant que membre d'une équipe et le chef d'équipe potentiels.
À la fin du programme, le participant :

- sera plus conscient des types de personnalité, préférences des personnes, leurs besoins, motivations et points forts
- comprendra ses propres préférences et besoins et capable de développer des buts dans plusieurs étapes de la vie/carrière d'apprécier la diversité culturelle au sein des équipes ; comprendre le rôle d'un chef d'équipe et membre de l'équipe
- aura reçu une gamme d'outils pour aider le participant à effectuer bien au sein d'une équipe et dans leur vie,
- obtiendra une vue d'ensemble comment les organisations et les personnes apprendre et développer d'élaborer un plan de carrière et la vie qui combine vos points forts et besoins, pour créer la crédibilité pour atteindre les objectifs

ENTREPRENARIAT ET CAPITAL-RISQUE

Ce cours est conçu pour familiariser les étudiants avec les défis associés à la création et au financement de la création d'entreprise. Son contenu inclut les décisions clés que l'entrepreneur doit prendre ainsi que la gestion des relations entre lui et la société de capital-risque. Comment trouver un accord ? Quelles sont leurs stratégies respectives ? Quel est le processus ?

CONTENU

- Créer votre propre entreprise
- Analyse du produit et du plan d'affaires
- Les sources de financement
    - L'environnement du capital risque
- Les critères d'investissement
- Les modèles de financement
- Les stratégies de croissance et de financement
- Faire des présentations orales efficaces
    - Valorisation et sorties
- Comprendre les « terms & conditions »
- Les actionnaires et les ouvertures de capital
- Les négociations

GESTION DE PROJET

Quel que soit le domaine considéré, les activités à effectuer sont, de plus en plus souvent, organisées en projets formels. Cette tendance est renforcée aujourd'hui dans un environnement

qui devient plus international et dans lequel les entreprises sont de plus en plus interdépendantes, notamment avec l'externalisation de tâches ou de fonctions entières. La communication à l'intérieur et à l'extérieur de l'entreprise joue un rôle crucial dans ce contexte. Afin de maîtriser efficacement ces projets, les entreprises font évoluer leur organisation d'un modèle fonctionnel vers un modèle matriciel, où le métier de Chef de Projet (Project Manager) devient essentiel. Ce cours a pour objectif d'initier les étudiants, aux différentes notions et techniques de conduite de projet, afin de leur faciliter l'insertion dans les équipes projet, de favoriser une compréhension plus globale des affaires et de déclencher une éventuelle réflexion sur leurs futures orientations professionnelles.

- Introduction : Les tendances sur le marché des technologies de l'information et des réseaux
- La notion de projet
- Les domaines du management de projets
- Genèse d'un projet : les demandes formelles
- La communication en entreprise
- Les modèles d'organisation
- Le périmètre
- Les coûts
- Le calendrier
- La Qualité
- La gestion des risques

INNOVATION ET DÉVELOPPEMENT DE PRODUITS NOUVEAUX

L'objectif de ce cours est de présenter le cadre de fonctionnement et les outils mis en place dans le développement de nouveaux produits. Les étudiants se familiariseront avec les procédés en jeu lorsqu'ils auront à faire face aux responsabilités inhérentes au développement de nouvelles technologies, produits ou services.

INTRODUCTION AU MANAGEMENT

La plupart des élèves ingénieurs auront, par ambition ou par nécessité, à un certain moment, dans leur carrière, des responsabilités de management. Ce cours va présenter aux étudiants la mission et la réalité du management du point de vue d'un futur jeune cadre. A travers des cours magistraux, des exercices et des études de cas, les étudiants comprendront and réaliseront ce qu'est la réalité quotidienne du manager aujourd'hui.

- Le rôle du manager : le management et les activités techniques, mythes et réalités, X, Y & Z, modèle Pareto de priorités
- Pourquoi les entreprises existent : stratégie, objectifs, retour sur investissement, équilibrer les attentes des différentes parties prenantes

- Mesurer et contrôler les activités d'une entreprise : comptabilité/finance/contrôle budgétaire, « balanced scorecards », outils d'aide à la décision
- Marketing et ventes
- Gestion des opérations : « business processes », PERT/CPM, MRP/ERP, TQM, Six sigma
- Théorie du capital humain

INTRODUCTION GÉNÉRALE AU DROIT : LES CONTRATS ET LA CRÉATION DE SOCIÉTÉ

Acquérir des connaissances juridiques dans le domaine de l'entreprise Avoir une vue d'ensemble concernant la création d'une société Connaître les grands principes du droit des contrats

Introduction générale du droit des contrats

I- Introduction générale : Présentation de la matière et définitions essentielles du droit

II- Les contrats : Présentation des contrats / Règles de formation d'un contrat / Clauses essentielles / Clauses fréquentes et leurs conséquences

La création d'une société

I- Introduction au droit des sociétés : Présentation du droit des sociétés / Présentation des différents types de structures : avantages/inconvénients

II- Les formalités de création d'une société : Aspects juridiques / Aspects financiers / Aspects fiscaux

III- Introduction à la propriété industrielle : Protéger sa marque / Protéger son domaine / Présentation du droit des brevets et logiciels

PROPRIÉTÉ INTELLECTUELLE

Le bus de ce cours est de connaître les principes fondamentaux de la propriété intellectuelle. Savoir détecter et anticiper les risques.
Introduction générale au droit de la propriété intellectuelle

1. La propriété littéraire et artistique

Eléments de compréhension du droit d'auteur et des droits voisins
Les conditions de la protection
Les conditions d'exploitation

2. Le droit des marques

Critères juridiques de choix d'une marque
Valorisation & défense de la marque

3. Le droit des brevets

Introduction et histoire du droit des brevets
Les conditions de brevetabilité
Les formalités auprès des offices
L'exploitation des brevets
Les brevets concernant les méthodes commerciales

4. Le droit des logiciels

SIMULATION D'ENTREPRISE

Grâce à l'utilisation d'une simulation complexe et interactive dans laquelle des équipes gèrent des entreprises virtuelles, les étudiants apprendront la pratique de la gestion. A la différence des autres cours, cette simulation requiert que les étudiants prennent des décisions en tenant compte de ses différents aspects (pluri-disciplinaires). Les étudiants comprendront aussi l'interdépendance entre les entreprises impliquées dans la simulation en termes d'achat-vente, de négociations, de partage de risque dans un environnement changeant.

- Application pratique des disciplines du management dans un environnement intégré et interactif (interaction entre les équipes).
- Exposition aux techniques de base du management (stratégie, comptabilité/finance, opérations, etc.…) dans le contexte de la prise de décision.
- Interprétation de l'environnement économique et son impact sur la performance future de l'entreprise.
- Application pratique des compétences managériales.
- Compréhension de l'importance des processus de gestion, notamment en matière de prise de décision.
- Expérience de la concurrence et de la coopération.

CONTACTS

RESPONSABLE DU DIPLÔME D'INGÉNIEUR DE SPÉCIALISATION :

Aurélien FRANCILLON
Aurelien.francillon@eurecom.fr

CANDIDATURE ET ADMISSION :

Caroline HANRAS
Caroline.hanras@eurecom.fr
+33 (0)4 93 00 81 33

POUR CANDIDATER

- Dossier de candidature en ligne : http://www.eurecom.fr/sifi/admission/
- Entretien téléphonique / Skype
- Guide de candidature disponible en ligne.

INFORMATION

Plus d'informations sur le site d'EURECOM :
http://www.eurecom.fr/fr/les-formations/ingenieur-de-specialisation/securite-des-systemes-informatiques-et-des-communications