الجمهورية الجزائرية الديمقراطية الشعبية
République Algérienne Démocratique et Populaire
وزارة التعليم العالي والبحث العلمي
Ministère de l'Enseignement Supérieur et de la Recherche Scientifique

Université Blida1
Faculté des Sciences

جامعة البليدة1
كلية العلـوم

B.P 270 Route de Soumâa – Blida
Tel : 025 27 24 52

Pr. Abed Bouarfa Hafida
Département d'informatique
Faculté des Sciences
Université Blida1
Tél : 0555184221

Blida le 25 Février 2024

A Monsieur le Président du Comité Pédagogique National du Domaine Mathématique-Informatique

Objet : Amendement du canevas de la formation de master Sécurité des SI

Le comité pédagogique de la formation master Sécurité des systèmes d'information ainsi que le chef du département d'informatique sollicitent Mr le Président du Comité Pédagogique National du Domaine Mathématique-Informatique afin qu'il valide leur demande d'amendement du canevas de la formation qu'ils assurent.

En fait, le master Sécurité des systèmes d'information est enseigné au niveau du département d'informatique de l'université de Blida depuis 2016. Cependant, nul n'ignore que la sécurité informatique est aujourd'hui une priorité absolue pour chaque entreprise et organisation. Le volume de données que les entreprises créent, manipulent et stockent ne cesse de croître, ce qui rend la bonne gouvernance des données plus nécessaire que jamais. De surcroît, les environnements informatiques sont plus complexes qu'autrefois car ils englobent désormais le cloud public, le centre de données de l'entreprise et de nombreux dispositifs périphériques comme les capteurs de l'Internet des objets (IoT), ou des serveurs distants. Cette complexité augmente la taille du périmètre à surveiller et à sécuriser face aux attaques potentielles.

Parallèlement, les individus sont de plus en plus sensibles aux questions de confidentialité des données et comprennent son importance. Répondant aux attentes du public, de nombreuses réglementations ont récemment été

adoptées en matière de protection de la vie privée. A cette issue, nous proposons un nouveau cours intitulé « Aspects juridique dans la sécurité informatique »

La donnée enregistre une croissance vertigineuse : le volume de data géré par les entreprises double tous les deux ans. Et cette tendance s'accélère. En parallèle, le niveau de risque augmente exponentiellement. Les individus malveillants se renforcent et poursuivent leurs activités de déstabilisation.

Dans ce contexte, la sécurité des données constitue l'un des enjeux majeurs auxquels font face les organisations qui manipulent des informations personnelles, sensibles ou stratégiques.

Il est en effet primordial d'assurer la protection de ces données contre les accès non autorisés, les violations, les attaques cyber et les cas de négligence humaine – autant d'événements susceptibles de nuire à l'entreprise, avec un coût financier (et surtout réputationnel) particulièrement élevé. Dans ce contexte, nous proposons de rajouter un nouveau module intitulé « Sécurité des applications »

Un défi d'autant plus complexe que les données sensibles sont désormais fragmentées, réparties sur l'ensemble du système d'information et des applications (machines et serveurs, services de Cloud public ou privé, infrastructure locale de type Edge, etc.). A cet effet, nous proposons de rajouter un module intitulé « Audit des systèmes d'information »

Pour toutes ces raisons, il est important pour nous de revoir les programmes afin de permettre à nos étudiants d'être au diapason de ce qui se fait ailleurs. Leur offrir un enseignement de base qui leur permettra de suivre l'évolution de l'informatique de manière générale et la sécurité des systèmes d'information de manière particulière. Les contenus des modules « Algorithmiques Avancés » et « systèmes d'exploitation » ont donc été enrichis.

Un module d'intelligence artificielle a été rajouté au programme. En fait, grâce à elle, les outils de cybersécurité sophistiqués sont capables d'analyser d'énormes ensembles de données, ce qui leur permet de développer des modèles d'activité pouvant détecter d'éventuels comportements malveillants et en alerter rapidement la Sécurité informatique.

Pr. Abed Bouarfa Hafida

REPUBLIQUE ALGERIENNE DEMOCRATIQUE ET POPULAIRE

MINISTERE DE L'ENSEIGNEMENT SUPERIEUR ET DE LA RECHERCHE SCIENTIFIQUE

CANEVAS D'AMENDEMENT

OFFRE DE FORMATION L.M.D.

MASTER ACADEMIQUE

Etablissement	Faculté / Institut	Département
Université de Blida 1	Sciences	Informatique

Domaine	Filière	Spécialité
M. I	Informatique	Sécurité des systèmes d'information

Responsable de l'équipe du domaine de formation :

Pr.Chellali Mustapha

الجمهورية الجزائرية الديمقراطية الشعبية
وزارة التعليم العالي و البحث العلمي

مواءمة

عرض تكوين ماستر

أكاديمي

المؤسسة	الكلية/ المعهد	القسم
جامعة البليدة 1	العلوم	الاعلام الالي

ا لميدان : رياضيات و اعلام الالي

الشعبة : اعلام الالي

التخصص : أمن نظم المعلومات

مسؤول فرقة ميدان التكوين:
شلالي مصطفى

SOMMAIRE

SOMMAIRE

I – Fiche d'identité du Master
(Tous les champs doivent être obligatoirement remplis)

1 - Localisation de la formation :

Faculté (ou Institut) : Sciences
Département : Informatique

2- Coordonateurs :

- Responsable de l'équipe du domaine de formation

Nom & prénom : CHELLALI Mustapha

Grade : Professeur
☎ : 025 27 24 17 Fax : 025 27 24 17 E - mail : m_chellali@yahoo.com

Joindre un CV succinct en annexe de l'offre de formation (maximum 3 pages)

- Responsable de l'équipe de la filière de formation

Nom & prénom : : FAREH Messaouda
Grade : Maître de conférences Classe A
☎ :025 27 24 17 Fax : 025 27 24 17 E - mail : farehm@univ-blida.dz
Joindre un CV succinct en annexe de l'offre de formation (maximum 3 pages)

- Responsable de l'équipe de spécialité

Nom & prénom : Bouarfa Abed Hafida Grade : Professeur
☎ : 0555184221 Fax : 025 27 24 17 e-mail : hafi.bouarfa@gmail.com
Joindre un CV succinct en annexe de l'offre de formation (maximum 3 pages)

Partenaires de la formation *:

- autres établissements universitaires :
- entreprises et autres partenaires socio économiques :
- Partenaires internationaux :

* = Présenter les conventions en annexe de la formation

3– Contexte et objectifs de la formation

A – Conditions d'accès *(indiquer les spécialités de licence qui peuvent donner accès au Master)*

Licence dans la filière Informatique et étude de dossier.

B - Objectifs de la formation *(compétences visées, connaissances acquises à l'issue de la formation- maximum 20 lignes)*

L'objectif est de former des spécialistes et chercheurs en sécurité des systèmes informatiques capables de concevoir, d'analyser et de mettre en œuvre des politiques de sécurité adaptées à différents environnements.
La recherche demandée dans ce domaine a clairement un caractère appliqué. Pour cette raison, la formation prévoit outre les disciplines théoriques nécessaires pour modéliser et résoudre les problèmes posés, un certain nombre de cours qui permettent d'appréhender de manière approfondie les aspects pratiques de la sécurité.

C – Profils et compétences métiers visés *(en matière d'insertion professionnelle - maximum 20 lignes) :*

Les diplômés du parcours peuvent utiliser leurs compétences dans le domaine de la recherche et du développement puisqu'ils ont une approche fondamentale permettant :

- A certains d'entre eux, s'ils le souhaitent, de préparer une thèse de doctorat à l'université.
- A d'autres, d'assurer au sein d'entreprises, des fonctions de responsable, de consultant de sécurité (CSSI, RSSI, DSSI), de chef de projet sécurité ou de concepteur_ développeur.

Les compétences visées sont :

- Concevoir et mettre en œuvre des politiques de sécurité dans des environnements variés.
- Analyser la vulnérabilité et les potentialités de sécurisation d'une infrastructure ; détecter ses failles et marges d'amélioration.
- Modéliser les problèmes de sécurité des données, du matériel, des réseaux, des systèmes d'exploitation et des applications.
- Réagir aux attaques, réparer un système endommagé.
- Identifier les origines d'un dommage ; fiabiliser les systèmes de détection, d'intrusion et de sauvegarde.
- Préconiser et fournir des solutions équilibrées tenant compte des contraintes techniques, organisationnelles, relationnelles.
- Convaincre les décideurs et les utilisateurs de l'importance des risques encourus et du bien-fondé des procédures envisagées ou déjà en cours.
- Organiser l'implémentation des décisions politiques, réglementaires, techniques (concernant la sécurité informatique) auprès de tout type d'utilisateur.
- Assurer une veille technologique sur les évolutions en matière de risques et de parades.

D- Potentialités régionales et nationales d'employabilité des diplômés

Toute entreprise ou organisation ou la sécurité informatique s'avère essentielle :

- Banques
- Assurances
- Sociétés de service en informatique générale
- Groupes industriels
- Collectivités
- Universités et centres de recherche

E – Passerelles vers les autres spécialités

F – Indicateurs de suivi de la formation

- Analyse quantitative et qualitative des résultats obtenus par les étudiants
- Niveau de participation des étudiants aux séminaires et conférences nationaux
- Niveau de participation et d'intégration des étudiants au développement des thèmes du laboratoire de recherche du département d'informatique.

G – Capacité d'encadrement (donner le nombre d'étudiants qu'il est possible de prendre en charge) :15

H- Equipe d'encadrement de la formation :

Enseignant	Diplôme graduation + Spécialité	Diplôme Post graduation + Spécialité	Grade	Typed'intervention	Emargement
ABED HAFIDA	Ingénieur d'état en informatique	Doctorat d'État Inffirmatique	PROF	Cours TD + Encadrement	
ARKAM MERIEM	Ingénieur d'état en informatique	Magistère Informatique	MAA	Cours TD +TP + Encadrement	
AROUSSI SANA	Ingénieur d'état en informatique	Magistère Informatique	MAA	Cours TD +TP + Encadrement	
BACHA SIHEM	Master en informatique	Magistère Informatique	MCB	Cours TD +TP + Encadrement	
BALA MAHFOUD	Ingénieur d'état en informatique	Doctorat Informatique	MCB	Cours TD +TP + Encadrement	
BENAISSI SALAMI	Ingénieur d'état en informatique	Magistère Informatique	MAB	Cours TD +TP + Encadrement	
BENYAHIA MOHAMED	Ingénieur d'état en informatique	Magistère Informatique	MAA	Cours TD +TP + Encadrement	
BERRAMDANE DJAMILA	Ingénieur d'état en informatique	Magistère Informatique	MAA	Cours TD +TP + Encadrement	
BEY FELLA	Master en informatique	Doctorat LMD en Informatiqu	MAB	Cours TD +TP + Encadrement	
BOUMAHDI FATIMA	Ingénieur d'état en informatique	Doctorat Informatique	MCB	Cours TD +TP + Encadrement	
BOUSTIA NARIHMENE	Ingénieur d'état en informatique	Doctorat Informatique	PROF	Cours TD + Encadrement	
BOUTOUMI BACHIRA	Ingénieur d'état en informatique	Magistère Informatique	MAA	Cours TD +TP + Encadrement	
CHERFA IMENE	Ingénieur d'état en informatique	Magistère Informatique	MAA	Cours TD +TP + Encadrement	
ERIF ZAHAR SID AMED AMI	Ingénieur d'état en informatique	Magistère Informatique	MAA	Cours TD +TP + Encadrement	
CHERIGUENE SOURAYA	Master en informatique	Doctorat LMD en Informatique	MAB	Cours TD +TP + Encadrement	
CHIKHI FATEH NACIM	Ingénieur d'état en informatique	Doctorat en Intelligence Artificielle	MCA	Cours TD +TP + Encadrement	
CHIKHI IMENE	Ingénieur d'état en informatique	Magistère Informatique	MAA	Cours TD +TP + Encadrement	
DJEDDAR AFRAH	Master en informatique	Doctorat LMD en Informatique	MCB	Cours TD +TP + Encadrement	
DOUGA YASSINE	Master en informatique	Doctorat LMD en Informatique	MCB	Cours TD +TP + Encadrement	
FAREH MESSAOUDA	Ingénieur d'état en informatique	Doctorat Informatique	MCB	Cours TD +TP + Encadrement	
FERFERA SOFIANE	Ingénieur d'état en informatique	Magistère Informatique	MAA	Cours TD +TP + Encadrement	
GHEBGHOUB YASMINE	Master en informatique	Doctorat LMD en Informatique	MCB	Cours TD +TP + Encadrement	
GUESSOUM DALILA	Ingénieur d'état en informatique	Magistère Informatique	MAA	Cours TD +TP + Encadrement	
HADJ HENNI MALIKA	Ingénieur d'état en informatique	Magistère Informatique	MAA	Cours TD +TP + Encadrement	
HAMMOUDA MOHAMED	Ingénieur d'état en informatique	Magistère Informatique	MAA	Cours TD +TP + Encadrement	
AMECHE ABDALLAH HICHA	Ingénieur d'état en informatique	Magistère Informatique	MAB	Cours TD +TP + Encadrement	
LAHIANI NESRINE	Master en informatique	Doctorat LMD en Informatique	MAB	Cours TD +TP + Encadrement	
MANCER YASMINE	Ingénieur d'état en informatique	Magistère Informatique	MAA	Cours TD +TP + Encadrement	
MESKALDJI KHOULOUD	Ingénieur d'état en informatique	Magistère Informatique	MAA	Cours TD +TP + Encadrement	
MEZZI MELYARA	Master en informatique	Doctorat LMD en Informatique	MCB	Cours TD +TP + Encadrement	
NASRI AHLEM	Master en informatique	Doctorat LMD en Informatique	MAB	Cours TD +TP + Encadrement	
NEHAL DJILALI	Ingénieur d'état en informatique	Magistère Informatique	MAA	Cours TD +TP + Encadrement	

OUAHRANI LEILA	Ingénieur d'état en informatique	Magistère Informatique	MAA	Cours TD +TP + Encadrement	
OUKID LAMIA	Master en informatique	Doctorat LMD en Informatique	MCB	Cours TD +TP + Encadrement	
OUKID SALIHA	Ingénieur d'état en informatique	Doctorat Informatique nouveau systeme	PROF	Cours + Encadrement	
OULD AISSA AHMED	Ingénieur d'état en informatique	Magistère Informatique	ASSISTANT	Cours TD +TP + Encadrement	
OULD KHAOUA MOHAMED	Ingénieur d'état en informatique	Doctorat Informatique	PROF	Cours TD + Encadrement	
TOUBALINE NESRINE	Ingénieur d'état en informatique	Doctorat Informatique	MCB	Cours TD +TP + Encadrement	
YKHLEF HADJER	Master en informatique	Doctorat LMD en Informatique	MCB	Cours TD +TP + Encadrement	
ZAHRA FATMA ZOHRA	Ingénieur d'état en informatique	Magistère Informatique	MAA	Cours TD +TP + Encadrement	

5 – Moyens matériels disponibles

A- Laboratoires Pédagogiques et Equipements : Fiche des équipements pédagogiques existants pour les TP de la formation envisagée (1 fiche par laboratoire)

Intitulé du laboratoire : TP Réseaux, Sécurité Réseaux

N°	Intitulé de l'équipement	Nombre	Observations
01	Câbles de paires torsadées souple	500m	
02	Câbles de paires torsadées rigide	2000 m	
03	Fibre optique Monomode	1000 m	
04	Connecteurs RJ45	500	
05	Connecteurs FO ST/SC	50	
06	Pince à sertir RJ45/RJ11	5	
07	Valise pour Collage Fibre Optique	3	
08	Valise pour Sertissage Paire Torsadée	1	
09	Fusionneuse de Fibre Optique	1	
10	PABX 4/16	1	
11	Modem Analogique externes	4	
12	Convertisseurs 100Base FX/100 Base TX	3	
13	Convertisseurs 1000 Base LX/1000 Base TX	3	
14	Testeurs Connexion RJ45	1	
15	Prise Murales RJ45	20	
16	Compatible PC + Onduleurs (en Réseau)	24	
17	Serveur	1	

B- Terrains de stage et formation en entreprise :

Lieu du stage	Nombre d'étudiants	Durée du stage
Elit, Oued Smar, Alger	4	03 Mois
CDTA, Baba Hassen	4	03 Mois
CERIST, Alger	4	03 Mois
ARPT, Alger	3	03 Mois

C- Laboratoire(s) de recherche de soutien à la formation proposée :

Benblidia Nadjia
Crée en mai 2002
Avis Favorable 

D- Projet(s) de recherche de soutien au master :

Intitulé du projet de recherche	Code du projet	Date du début du projet	Date fin du projet
Représentation et raisonnement des connaissances à partir des données liées	C00L09UN090120220001	Janvier 2022	Décembre 2025
Architectures Neuronales pour la détection visuelle/textuelle du cancer du sein à partir des données massives	C00L07UN090120220002	Janvier 2022	Décembre 2025
Sécurité des réseaux sociaux	C00L07UN090120220003	Janvier 2022	Décembre 2025

E- Espaces de travaux personnels et TIC :

- Bibliothèque centrale
- Bibliothèque Faculté des Sciences

II – Fiche d'organisation semestrielle des enseignements

(Prière de présenter les fiches des 4 semestres)

1- Semestre 1 :

Unité d'Enseignement	VHS	V.H hebdomadaire				Coeff	Crédits	Mode d'évaluation	
	14-16 sem	C	TD	TP	Autres			Continu	Examen
UE fondamentales									
UEF1									
Algorithmique Avancé	67h30	1h30	1h30	1h30		3	6	X	X
Réseaux	67h30	1h30	1h30	1h30		3	6	X	X
Administration de bases de données	67h30	1h30	1h30	1h30		3	6	X	X
UE Méthodologique									
UEM1									
Cryptographie	67h30	1h30	1h30	1h30		3	6	X	X
Programmation C++	45h		1h30	1h30		2	3	X	X
UE découverte									
UED1									
Recherche Opérationnelle	22h30	1h30				1	1	X	X
UE transversales									
UET1									
Intelligence Artificielle	22h30	1h30				1	1	X	X
Cybercriminalité	22h30	1h30				1	1	X	X
Total Semestre 1	382h30					17	**30**		

2- Semestre 2

Unité d'Enseignement	VHS	V.H hebdomadaire				Coeff	Crédits	Mode d'évaluation	
	14-16 sem	C	TD	TP	Autres			Continu	Examen
UE fondamentales									
UEF2									
Systèmes d'exploitation	67h30	1h30	1h30	1h30		3	6	X	X
Applications distribuées	67h30	1h30	1h30	1h30		3	6	X	X
Réseaux avancés	67h30	1h30	1h30	1h30		3	6	X	X
UE Méthodologique									
UEM2									
Initiation à la sécurité	45h	1h30		1h30		2	4	X	X
Sécurité des applications	67h30	1h30	1h30	1h30		3	5	X	X
UE transversales									
UET2									
Audit des SI	22h30	1h30				1	1	X	X
Aspects juridiques dans la sécurité informatique	22h30	1h30				1	1	X	X
Entreprenariat	22h30	1h30				1	1	X	X
Total Semestre 2	382h30					17	**30**		

3- Semestre 3 :

Unité d'Enseignement	VHS	V.H hebdomadaire				Coeff	Crédits	Mode d'évaluation	
	14-16 sem	C	TD	TP	Autres			Continu	Examen
UE fondamentales									
UEF3									
Sécurité des systèmes d'information	67h30	1h30	1h30	1h30		3	6	X	X
Sécurité des réseaux	67h30	1h30	1h30	1h30		3	6	X	X
Sécurité des bases de données	67h30	1h30	1h30	1h30		3	6	X	X
UE Méthodologique									
UEM3									
Méthodologie de la sécurité	45h	3h				2	4	X	X
Techniques de gestion des identités	22h30	1h30				1	1	X	X
Méthodologie avancée de la sécurité	45h	1h30	1h30			2	4	X	X
UE transversales									
UET3									
Gestion de projets	45	1h30	1h30			2	2	X	X
Techniques de rédaction	22h30	1h30				1	1	X	X
Total Semestre 3	382h30					17	**30**		

4- Semestre 4 :

Domaine : Mathématique / Informatique
Filière : Informatique
Spécialité : Sécurité des Systèmes Informatiques

Stage en entreprise sanctionné par un mémoire et une soutenance.

	VHS	Coeff	Crédits
Travail Personnel			
Stage en entreprise			
Séminaires			
Mémoire fin d'étude	375h	1	30
Total Semestre 4	375h	1	30

5- Récapitulatif global de la formation : (indiquer le VH global séparé en cours, TD, pour les 04 semestres d'enseignement, pour les différents types d'UE)

UE / VH	UEF	UEM	UED	UET	Total
Cours	202.5	157.5	22.5	180	
TD	202.5	90			
TP	202.5	90			
Travail personnel					
Mémoire Fin Etude	375				
Total	982.5	337.5	22.5	180	
Crédits	84	27	1	8	**120**
% en crédits pour chaque UE	70%	22%	0.84%	6.66%	100%

IV - Programme détaillé par matière

(1 fiche détaillée par matière)

Intitulé du Master : Sécurité des systèmes d'information

Semestre *:* 1
Intitulé de l'UE : UEF1
Intitulé de la matière : Algorithmique Avancé
Crédits : 6
Coefficients :3

Objectifs de l'enseignement (*Décrire ce que l'étudiant est censé avoir acquis comme compétences après le succès à cette matière – maximum 3 lignes).*

- *Apprendre à effectuer une analyse formelle des algorithmes basée sur leurs complexités temporelle et spatiale.*
- *Evaluer l'efficacité des solutions (algorithmes de résolution) avant même de les implémenter, une étape nécessaire dans la résolution de n'importe quel problème.*
- *Classifier les problèmes selon leur degré de complexité.*
- *Utiliser des méthodes approchées pour résoudre les problèmes complexes.*

Connaissances préalables recommandées (*descriptif succinct des connaissances requises pour pouvoir suivre cet enseignement – Maximum 2 lignes).*

- *Algorithmique et structure de données.*
- *Théorie de la programmation.*
- *Théorie des graphes.*

Contenu de la matière :

1- La complexité de calcul

a. Exemples introductifs
b. Algorithme et complexité
c. Complexité théorique : Complexité temporelle vs complexité spatiale
d. Complexité temporelle.
    Définition et notion de landau
    Règles de calcul
    Classes de complexité

2. Structures de données élémentaires et avancées

a. Introduction aux structures de données
b. Rappel sur les structures de données élémentaires
    Listes chainées
    Les Piles
    Les files
c. Structures de données avancées
    Les arbres binaires et les arbres binaires de recherche
    Les arbres binaires équilibrés : structure du TAS, AVL
    Les arbres M-aire de recherche et M-aire de recherche équilibré

3. Techniques de conception d'algorithmes

a. La récursivité
b. Technique 'Diviser et Conquérir'
c. La programmation dynamique

4. Algorithmes de tri (Fait comme TP – Partie calcul de complexité dont le but est de comparer la complexité théorique et expérimentale des différents algorithmes de Tri)

a. Les algorithmes classiques de tri (tri Sélection, Tri par Insertion, Tri à Bulles)
b. Les algorithmes de tri plus performants (Le tri Rapide, le tri par Tas, le tri Fusion)

5. Les algorithmes de graphe.

a. Rappels et notions élémentaires
b. Parcours d'un arbre (graphe)
    Parcours en profondeur d'abord
    Parcours en largueur d'abord
c. Recherche du plus court chemin
    Algorithme de Djikstra
d. Arbre couvrant de poids minimal
    Algorithme de Kruskal

6. Introduction à la NP-complétude

a. Introduction et notions fondamentales
b. Problème, Instance de problème et solution
c. Types de problèmes (Décision, Optimisation, Dénombrement de solutions…)
d. Classes de problèmes
    La classe P
    La classe NP
    La classe NP-complet

Mode d'évaluation : Examens Ecrits (60%) + Contrôle continu (40%)

Références : *Livres et polycopiés, sites internet, etc).*

- Patrick Siarry, Johann Dréo, Alain Pétrowski, Éric Taillard : Métaheuristiques pour L'optimisation difficile, Eyrolles, 2003
- Eléments d'algorithmique Auteur(s) Beauquier, Danièle; Berstel, Jean; Chrétienne, Philippe. Edition masson 2003.
- Computers and Intractability: A Guide to the Theory of NP-Completeness (Michael R. Gareyand and David S. Johnson) 2006.

Intitulé du Master : Sécurité des systèmes d'information

Semestre *:* 1
Intitulé de l'UE : UEF1
Intitulé de la matière : Réseaux
Crédits : 6
Coefficients :3

Objectifs de l'enseignement (*Décrire ce que l'étudiant est censé avoir acquis comme compétences après le succès à cette matière – maximum 3 lignes).*

Développer certaines notions avancées sur les réseaux telles que le protocole IPv6, le routage dynamique et les réseaux WiFi 802.11

Connaissances préalables recommandées (*descriptif succinct des connaissances requises pour pouvoir suivre cet enseignement – Maximum 2 lignes).*

Contenu de la matière :

- Rappels sur la couche physique
- Rappels sur la couche MAC : CSMA/CD
- Etude des réseaux WIFI 802.11
- Ethernet commuté, algorithme d'un commutateur, Spanning Tree Protocol, VLAN
- IP approfondi (fragmentation, ICMP, IP multicast)
- Introduction aux protocoles de routage dynamique RIP, OSPF, aux systèmes autonomes et BGP
- TCP approfondi : les différents algorithmes de gestion de la congestion
- IPv6
- Introduction au NAT
- Introduction au pare-feu et au proxy
- Programmation sockets avancée, IPV6
- FTP actif et passif, RPC, NFS, DNS avancé, …

Mode d'évaluation : *(2 × note examen final + note contrôle continu) / 3*

Références (*Livres et polycopiés, sites internet, etc).*

- Andrew Tanenbaum and David J.Wetherall. *Réseaux*. Pearson, 5ème édition, 2011.
- Guy Pujolle. *Les réseaux*. Eyrolles, 8ème édition, 2014.

Intitulé du Master : Sécurité des systèmes d'information

Semestre *:* 1
Intitulé de l'UE : UEF1
Intitulé de la matière : Administration des BDD
Crédits : 6
Coefficients :3

Objectifs de l'enseignement (*Décrire ce que l'étudiant est censé avoir acquis comme compétences après le succès à cette matière – maximum 3 lignes).*

Ce cours a pour objectif d'initier les étudiants à l'administration des bases de données. Les étudiants apprendront à installer, configurer et maintenir un SGBD. Ils seront sensibilisés aux enjeux de la disponibilité et de la sécurité de ceux-ci. Ils verront également quelles sont les tâches les plus fréquentes à réaliser dans le métier de DBA. A l'issue du cours, l'étudiant sera en mesure de :

• Installer, designer et gérer un SGBD de façon adéquate aux besoins
• Sécuriser les fichiers critiques
• Manipuler et migrer des données
• Sauvegarder et restaurer
• Sécuriser les données
• Surveiller et maintenir

Connaissances préalables recommandées (*descriptif succinct des connaissances requises pour pouvoir suivre cet enseignement – Maximum 2 lignes).*
Connaissances des concepts théoriques des bases de données et du langage SQL

Contenu de la matière :

1. **Introduction à l'administration des bases de données**
2. **Gestion des transactions et accès concurrents**
   a. Transaction et primitives
   b. Propriétés ACID
   c. Ordonnancement et Sérialisabilité
   d. Contrôle des accès concurrents
   e. Gestion des transactions pour les BDD réparties
3. **Gestion des utilisateurs et l'architecture de sécurité**
   a. Gestion des utilisateurs et de leurs droits
   b. Gestion de sécurité
4. **Gestion de stockage et reprise après panne**
   a. Le dictionnaire et catalogue de données
   b. Gestion des fichiers disques et les données d'annulation
   c. Gestion des espaces disque logiques
   d. Sauvegarde et récupération

5. **Optimisations de requêtes**

a. Généralités sur l'optimisation des requêtes
b. Traduction de la requête SQL en algèbre relationnelle
c. Calculer les coûts des plans

Mode d'évaluation : Examens Ecrits (60%) + Contrôle continu (40%)

Références *(Livres et polycopiés, sites internet, etc.).*

[1] Nacer BOUDJLIDA. livre : Gestion et administration des bases de données. Dunod. ISBN-13 : 978-2100058471, 2003.
[2] OLIVIER CURE. Polycopié de cours : Concurrence et transactions. Université de Marne la vallée de Paris, France.
[3] GARDARIN GEORGES. livre : Bases de données : Objet et relationnel. Eyrolles. ISBN-13 : 978-2212092837, 2001.
[4] CHANTAL GRIBAUMONT. livre : Administrez vos bases de données avec MySQL. OpenClassrooms. ISBN-13 : 979-1090085671, 2014.
[5] RICHARD GRIN. Polycopié de cours : Langage SQL. Institut Universitaire de Technologie de Villetaneuse de Nice, France.
[6] MAXIMILIEN LAURENT. Polycopié de cours : Concepts et langages des Bases de Données Relationnelles. Institut Universitaire de Technologie de Villetaneuse de Nice, France.

Intitulé du Master : Sécurité des systèmes d'information

Semestre *:* 1
Intitulé de l'UE : UEM1
Intitulé de la matière : Cryptographie
Crédits : 6
Coefficients :3

Objectifs de l'enseignement (*Décrire ce que l'étudiant est censé avoir acquis comme compétences après le succès à cette matière – maximum 3 lignes).*

Initier les étudiants aux principales techniques de cryptographie.

Connaissances préalables recommandées (*descriptif succinct des connaissances requises pour pouvoir suivre cet enseignement – Maximum 2 lignes).*

Contenu de la matière :

- Introduction générale
- Chiffrement à clé secrète
- Fonctions de hachage
- Chiffrement à clé publique
- Authentification de l'origine des messages (symétrique et asymétrique)
- Génération d'aléa cryptographique
- Exemples de protocoles cryptographiques

Mode d'évaluation : *(2 × note examen final + note contrôle continu) / 3*

Références (*Livres et polycopiés, sites internet, etc.).*

- Gilles Dubertret. *Initiation à la cryptographie : Cours et exercices corrigés*. Vuibert, 2012.
- Niels Ferguson, Bruce Schneier, Tadayoshi Kohno. *Cryptography Engineering: Design Principles and Practical Applications*. Wiley, 2010.

Intitulé du Master : Sécurité des systèmes d'information

Semestre *:* 1
Intitulé de l'UE : UED1
Intitulé de la matière : Optimisation et recherche opérationnelle
Crédits : 1
Coefficients :1

Objectifs de l'enseignement (*Décrire ce que l'étudiant est censé avoir acquis comme compétences après le succès à cette matière – maximum 3 lignes).*

Comprendre et modéliser un problème.

- Se familiariser avec les techniques de programmation linéaire - graphique et Algorithme du Simplexe
- Se familiariser avec les problèmes combinatoires
- Différencier les techniques de résolution classiques et intelligentes.
- Avoir les capacités de raisonner devant un problème complexe.
- Evaluer l'efficacité d'une solution.

Connaissances préalables recommandées (*descriptif succinct des connaissances requises pour pouvoir suivre cet enseignement – Maximum 2 lignes).*

- Algorithmique et structure de données
- Programmation
- Notions de base en théorie des graphes
- Algorithmique avancée
- NP-complétude

Contenu de la matière :

Partie I : Programmation linéaire

1. Modélisation d'un problème de programmation linéaire
2. Résolution graphique d'un problème de programmation linéaire
3. Résolution par l'algorithme du Simplexe d'un problème de programmation linéaire
4. Dualité en programmation linéaire
5. Programmation linéaire en nombre entier - Branch and Bound

Partie II : Optimisation Combinatoire

1. Rappel sur la NP-complétude (Voir cours Algorithmique avancée pour plus de détails)
2. Algorithmes Exactes pour la résolution de problèmes combinatoires
    - Exemples de problèmes combinatoires
    - Notions fondamentales à la résolution de problèmes
    - Méthodes de recherche aveugles
    - Méthodes heuristiques

3. Algorithmes approchés pour la résolution de problèmes combinatoires

- Algorithmes évolutionnaires
- Méta-heuristique et Intelligence en essaim
    - Introduction et type de méta-heuristique
    - Recherche locale et recherche taboue
    - Les algorithmes génétiques
    - Les essaims d'abeilles
    - Les colonies de fournis
    - L'hybridation entre méta-heuristique

Mode d'évaluation : Examens Ecrits (60%) + Contrôle continu (40%)

Références *(Livres et polycopiés, sites internet, etc.).*

- Gendreau, M., & Potvin, J. Y. (Eds.). (2010). Handbook of metaheuristics (Vol. 2, p. 9). New York: Springer.
- Faure, R., Lemaire, B., & Picouleau, C. (2014). Précis de recherche opérationnelle. Dunod (Paris 1979).
- Bellal, S. INTRODUCTION À LA RECHERCHE OPÉRATIONNELLE (OPU)

Intitulé du Master : Sécurité des systèmes d'information

Semestre *:* 1
Intitulé de l'UE : UET1
Intitulé de la matière : Intelligence Artificielle
Crédits : 1
Coefficients :1

Objectifs de l'enseignement (*Décrire ce que l'étudiant est censé avoir acquis comme compétences après le succès à cette matière – maximum 3 lignes).*

- Situer l'Intelligence Artificielle en tant que discipline scientifique
- Maîtriser les concepts de base de l 'intelligence artificielle
- Connaître les méthodes de représentation des connaissances
- Avoir un aperçu des approches pour la résolution de problèmes en IA

Connaissances préalables recommandées (*descriptif succinct des connaissances requises pour pouvoir suivre cet enseignement – Maximum 2 lignes).*

Les connaissances algorithmiques et éléments de logiques acquises en cours de formation « licence »

Contenu de la matière :

I. Introduction : une brève histoire de l'IA
II. L'IA et la résolution des problèmes
    a. Démarche IA pour résoudre un problème
    b. Démarches de construction de la solution o Résolution par décomposition en sous problèmes
    c. Résolution par satisfaction de contraintes
III. Les systèmes à base de connaissances
    a. Définition
    b. Architecture
    c. Ingénierie des connaissances
IV. Python : un langage pour l'IA

Mode d'évaluation : Examens Ecrits (60%) + Contrôle continu (40%)

Références (*Livres et polycopiés, sites internet, etc.).*

[1] Principles of Artificial Intelligence par J. Nilson
[2] Essentials of Artificial Intelligence par Morgan Kaufmann,
[3] Artificial Intelligence : A new synthesis par Morgan Kaufmann,
[4] Artificial Intelligence : A Modern Approach par Stuart Russell et Peter Norvig
aima.cs.berkeley.edu

Intitulé du Master : Sécurité des systèmes d'information

Semestre *:* 1
Intitulé de l'UE : UEM1
Intitulé de la matière : Programmation C++
Crédits : 3
Coefficients :2

Objectifs de l'enseignement (*Décrire ce que l'étudiant est censé avoir acquis comme compétences après le succès à cette matière – maximum 3 lignes).*

Etudier les principes de la programmation orientée objet et leur mise en œuvre en C++

Connaissances préalables recommandées (*descriptif succinct des connaissances requises pour pouvoir suivre cet enseignement – Maximum 2 lignes).*

Contenu de la matière :

- Rappel du paradigme orienté objet
- Les classes (constructeurs, destructeurs, accesseurs, opérateurs, pointeurs et références sur les objets)
- L'héritage (méthodes virtuelles et redéfinition, polymorphisme, liaisons dynamiques, classes abstraites)
- La surcharge des opérateurs en C++
- Librairies standard

Mode d'évaluation : *(2 × note examen final + note contrôle continu) / 3*

Références *(Livres et polycopiés, sites internet, etc).*

- Claude Delannoy. *Programmer en langage C++*. Eyrolles, 8ème édition, 2011.
- Bjarne Stroustrup. *The C++ Programming Language*. Addison Wesley, 4ème édition, 2013.

Intitulé du Master: Sécurité des systèmes d'information

Semestre *:* 2
Intitulé de l'UE : UEF2
Intitulé de la matière : Systèmes d'exploitation
Crédits : 6
Coefficients :3

Objectifs de l'enseignement (*Décrire ce que l'étudiant est censé avoir acquis comme compétences après le succès à cette matière – maximum 3 lignes).*

- Approfondir les notions de gestion des threads notamment l'ordonnancement, la synchronisation et la communication. Pour chaque notion,
- Mettre l'accent sur les aspects de sécurité (problèmes et solutions).
- Apprendre à programmer la solution avec la norme POSIX.

Connaissances préalables recommandées (*descriptif succinct des connaissances requises pour pouvoir suivre cet enseignement – Maximum 2 lignes).*

L'étudiant doit connaître les notions de bases sur la gestion des processus (lourds et légers), notamment : création, ressources nécessaires, politiques ordonnancement, partage de mémoire, synchronisation, [SE1 & SE2, 2ème et 3ème année Licence]

Contenu de la matière :

0. Introduction à la Sécurité des Systèmes d'Exploitation
1. Partie I : Rappel sur les processus, les threads et les Pthread (POSIX Thread)
2. Partie II : Ordonnancement
    - Ordonnancement des processus (lourds\légers)
        - Rappel sur les algorithmes d'ordonnancement classiques (avec une seule file d'attente)
        - Les algorithmes d'ordonnancement avec plusieurs files d'attente.
        - Cas d'étude : MS-DOS, WINDOWS, LINUX, UNIX
    - Ordonnancement des pthreads
    - Etude des aspects de sécurité liés aux politiques d'ordonnancement.
3. Partie III : Synchronisation
    - Rappel sur l'Exclusion Mutuelle
    - Mécanismes : Verrous, Sémaphores et Moniteurs
    - Problèmes classiques : Producteurs\Consommateurs ; Lecteurs/Rédacteurs, Rendez-vous, …
    - Etude des aspects de sécurité liés aux mécanismes de synchronisation.
    - Interblocage
4. Partie IV : Communication
    - Directes versus indirectes
    - Méthodes de communication : mailbox, pipe, sockets….

- Etude des aspects de sécurité liés aux mécanismes de communication.

Mode d'évaluation : *(2 × note examen final + note contrôle continu) / 3*

Références *(Livres et polycopiés, sites internet, etc.).*

- Andrew Tanenbaum. *Systèmes d'exploitation*. Pearson, 3ème édition, 2008.
- Thomas Anderson, Michael Dahlin. *Operating Systems: Principles and Practice*. Recursive Books, 2012.

Intitulé du Master : Sécurité des systèmes d'information

Semestre *:* 2
Intitulé de l'UE : UEM2
Intitulé de la matière : Initiation à la sécurité
Crédits : 4
Coefficients :2

Objectifs de l'enseignement (*Décrire ce que l'étudiant est censé avoir acquis comme compétences après le succès à cette matière – maximum 3 lignes).*

Initier et sensibiliser les étudiants à la sécurité informatique.

Connaissances préalables recommandées (*descriptif succinct des connaissances requises pour pouvoir suivre cet enseignement – Maximum 2 lignes).*

Contenu de la matière :

- Rappels de TCP/IP et IPv6
- Les pare-feu
- Les techniques de chiffrement des données
- Les protocoles sécurisés : IPSEC, DNSSEC, HTTPS, SSH, …
- Les types d'attaques ; les failles des systèmes et des applications, les audits de vulnérabilité

Mode d'évaluation : *(2 × note examen final + note contrôle continu) / 3*

Références *(Livres et polycopiés, sites internet, etc).*

- Laurent Bloch, Christophe Wolfhugel, Nat Makarévitch, Christian Queinnec, Hervé Schauer. *Sécurité informatique : Principes et méthodes à l'usage des DSI, RSSI et administrateurs*. Eyrolles, 4ème édition, 2013.
- Gildas Avoine, Pascal Junod, Philippe Oechslin. *Sécurité informatique : Cours et exercices corrigés*. Vuibert, 2ème édition, 2009.

Intitulé du Master : Sécurité des systèmes d'information

Semestre *:* 2
Intitulé de l'UE : UEF2
Intitulé de la matière : Applications distribuées
Crédits : 6
Coefficients :3

Objectifs de l'enseignement (*Décrire ce que l'étudiant est censé avoir acquis comme compétences après le succès à cette matière – maximum 3 lignes).*

Présenter les méthodes de communication dans les systèmes distribués et les techniques de mise en œuvre d'applications web.

Connaissances préalables recommandées (*descriptif succinct des connaissances requises pour pouvoir suivre cet enseignement – Maximum 2 lignes).*

Langages orientés objet, systèmes d'exploitation, compilation, réseaux et communication

Contenu de la matière :

Chapitre 1 : Mesure des performances
Chapitre 2 : Caractéristiques des systèmes distribués
Chapitre 3 : Les threads dans les systèmes distribués
- Synchronisation des threads en Java

Chapitre 4 : Protocoles de communication
Chapitre 5 : Communication dans les applications distribuées
- Communication à l'aide des sockets en Java

Chapitre 6 : Modèles d'architectures distribuées
- Architecture client-serveur
- Architecture peer-to-peer
- Architecture à micro-services

Chapitre 7 : Web avancé
- Architecture des applications web
- Modèle MVC
- Jakarta Enterprise Edition
- Création d'API avec Spring Boot

Chapitre 8 : Technologies actuelles pour les applications distribuées
- Conteneurisation (Docker, Kubernetes)
- Architectures serverless
  Blockchain

Mode d'évaluation : *(2 × note examen final + note contrôle continu) / 3*

Références *Livres et polycopiés, sites internet, etc.).*

- Maarten van Steen & Andrew S. Tanenbaum. Distributed Systems. Maarten van Steen, 2017.

- Mark Heckler. Spring Boot: Up and Running - Building Cloud Native Java and Kotlin Applications. O'Reilly Media, 2021.

- Irakli Nadareishvili, Ronnie Mitra, Matt McLarty & Mike Amundsen. Microservice architecture: Aligning Principles, Practices, and Culture. O'Reilly, 2016.

- Gabriel N. Schenker. The Ultimate Docker Container Book: Build, test, ship, and run containers with Docker and Kubernetes. Packt Publishing, 2023.

- John Gilbert. Software Architecture Patterns for Serverless Systems. Packt Publishing, 2023.

- Mary C. Lacity & Steven C. Lupien. Blockchain Fundamentals for Web 3.0. Epic Books, 2022.

Intitulé du Master : Sécurité des systèmes d'information

Semestre *:* 2
Intitulé de l'UE : UEF2
Intitulé de la matière : Réseaux avancés
Crédits : 6
Coefficients :3

Objectifs de l'enseignement (*Décrire ce que l'étudiant est censé avoir acquis comme compétences après le succès à cette matière – maximum 3 lignes).*

Etudier plus en détail certains aspects des réseaux liés à la sécurité tels que l'authentification PAM et les outils d'audit de vulnérabilité.

Connaissances préalables recommandées (*descriptif succinct des connaissances requises pour pouvoir suivre cet enseignement – Maximum 2 lignes).*

Contenu de la matière :

- Gestion de la journalisation (syslog et rsyslog)
- Les attaques par usurpations : spoofing et raw sockets
- Les outils d'audit de vulnérabilité – programmation de modules de détection de vulnérabilité et d'attaques
- L'authentification (PAM) : présentation, configuration et développement de modules PAM
- Les VPN et IPSEC
- La norme 802.1x et Radius

Mode d'évaluation : *(2 × note examen final + note contrôle continu) / 3*

Références *(Livres et polycopiés, sites internet, etc).*

- Richard Bejtlich. *The Practice of Network Security Monitoring: Understanding Incident Detection and Response.* No Starch Press, 2013.
- José Dordoigne. *Réseaux informatiques - Notions fondamentales (Protocoles, Architectures, Réseaux sans fil, Virtualisation, Sécurité, IP v6, ...)*. Editions ENI, 5ème édition, 2013.

Intitulé du Master : Sécurité des systèmes d'information

Semestre *:* 2
Intitulé de l'UE : UET2
Intitulé de la matière : Audit des systèmes d'information
Crédits : 1
Coefficients :1

Objectifs de l'enseignement (*Décrire ce que l'étudiant est censé avoir acquis comme compétences après le succès à cette matière – maximum 3 lignes).*

Permettre à l'étudiant d'acquérir des connaissances techniques dans les domaines de l'évaluation de performances, du diagnostic, de l'analyse des risques informatiques et du l'analyse de la valeur des systèmes d'information.

Connaissances préalables recommandées (*descriptif succinct des connaissances requises pour pouvoir suivre cet enseignement – Maximum 2 lignes).*

Pour suivre les enseignements dispensés dans cette matière, il est nécessaire que l'étudiant ait déjà eu au préalable des notions de systèmes d'information. .

Contenu de la matière :

Chapitre I : Introduction à l'Audit des Systèmes d'Information.
Chapitre II : Principes Généraux de L'audit Des Systèmes d'Information.
Chapitre III : Schéma Conceptuel De L'audit Des Systèmes D'information.
Chapitre VI : Les Référentiels De L'audit Des Systèmes D'information.

Mode d'évaluation : Examen (100%).

Références :

[1] Advisory, le conseil durable (2009), Efficacité et maitrise du système d'information, PWC, http://pwc.to/z0SjmD
[2] Ahmed Bounfour, Capital immatériel, connaissance et performance, Harmattan, 2006 (ISBN 978-2-2960-1128-1) p. 127
[3] Cadre de Référence International des Pratiques Professionnelles de l'audit interne, IIAIFACI, 2009.
[4] MOISAND D., GARNIER DE LABAREYRE F. (2009), CobiT : pour une meilleure gouvernance des systèmes d'information, Ed. Paris : Eyrolles, 274 pages.
[5] PETIT G., JOLY D. et MICHEL J. (1985), Audit et informatique : Guide pour l'audit financier des entreprises informatisées, Volume 1, Ed. Paris : CLET, 268 pages.
[6] TOURY A. (2006), Proposition d'une méthodologie pour la conduite des missions d'audit informatique, mémoire présenté pour l'obtention du diplôme national d'expertcomptable, ISCAE, 174 pages, http://bit.ly/xFoxoB

Intitulé du Master : Sécurité des systèmes d'information

Semestre *:* 2
Intitulé de l'UE : UEM2
Intitulé de la matière : Sécurité des applications
Crédits : 5
Coefficients :3

Objectifs de l'enseignement (*Décrire ce que l'étudiant est censé avoir acquis comme compétences après le succès à cette matière – maximum 3 lignes).*

L'objectif est de faire connaitre aux étudiants comment sécuriser une application, quels sont les véritables menaces et qu'elles sont les conséquences d'une mauvaise sécurisation des applications

Connaissances préalables recommandées (*descriptif succinct des connaissances requises pour pouvoir suivre cet enseignement – Maximum 2 lignes).*

Connaitre les notions fondamentales de la sécurité : Vulnérabilité des applications, les risques, les menaces existantes

Contenu de la matière :

1 Introduction à la sécurité sur le web
- 1 Risques et enjeux
- 2 Concepts de sécurité
- 3 Sécurité au niveau physique

2 Sécurité au niveau du système d'exploitation

3 Intégrité de l'application web
- 1 Vulnérabilités des pages HTML
- 2 Intégrité des scripts PHP
- 3 Risques causés par les données saisies par les utilisateurs
- 4 Téléchargement de fichiers vers le serveur (upload)
- 5 Risques liés aux cookies et sessions

4 Sécurité du SGBD
- 1 Injection de SQL
- 2 Accès au serveur
- 3 Accès secondaires

5 Chiffrement et signature des données
- Systèmes de chiffrement symétrique/asymétrique
- 2 Signature numérique
- 3 Certificats authentifiés
- 4 Infrastructure à clé publique (PKI)

6 Sécurité sur le réseau

1 Vulnérabilités du réseau

2 Sécurisation d'un ensemble de machines (segmentation en sous-réseaux, filtrage…)

3 Chiffrement des communications et authentification des tiers (SSL/TLS, tunneling SSH, IPSec, VPN)

Mode d'évaluation : *(2 × note examen final + note contrôle continu) / 3*

Références *(Livres et polycopiés, sites internet, etc.).*

-Sécurité PHP5 et MySQL, Damien Seguy et Philippe Gamache, Eyrolles, 2007.
- Pro PHP Security: From Application Security Principles to the Implementation of XSS Defenses 2nd edition, Chris Snyder, Thomas Myer and Michael Southwell, Apress, 2010.
- Sécurité Informatique Principes et méthode, Laurent Bloch et Christophe Wolfhugel, Eyrolles, 2007.
- Tableaux de bord de la sécurité réseau 2`eme édition, Cédric Llorens, Laurent Levier et Denis Valois, Eyrolles, 2006.
- Web Security Testing Cookbook, Paco Hope and Ben Walther, O'REILLY, 2008.

Intitulé du Master : Sécurité des systèmes d'information

Semestre : 2
Intitulé de l'UE : UET2
Intitulé de la matière : Entreprenariat
Crédits : 1
Coefficients : 1

Objectifs de l'enseignement : Cet Enseignement vise à initier l'apprenant au montage de projet, son lancement, son suivi et sa réalisation.

Connaissances préalables recommandées :

Contenu de la matière :

Chapitre 1 : L'étude du marché.

Chapitre 2 : Les opérations financières

Chapitre 3 : Gestion des achats,

Chapitre 4 : Gestion des stocks

Chapitre 5 : Mode de production,

Chapitre 6 : Politique de produits,

Chapitre 7 : Politique de prix,

Chapitre 8 : Publicité

Mode d'évaluation : Examen (100%).

Références

- Schmitt, Christophe. "La fabrique de l'entrepreneuriat." Dunod, Paris (2017).
- Julien, Pierre-André. La mesure de l'entrepreneuriat. des Libris, 2010.
- Léger-Jarniou, Catherine. Le grand livre de l'entrepreneuriat. Dunod, 2013.

Intitulé du Master : Sécurité des systèmes d'information

Semestre *:* 3
Intitulé de l'UE : UEM3
Intitulé de la matière : Méthodologie de la sécurité
Crédits : 4
Coefficients :2

Objectifs de l'enseignement (*Décrire ce que l'étudiant est censé avoir acquis comme compétences après le succès à cette matière – maximum 3 lignes).*

Initier les étudiants à la gestion du risque informatique et à la méthodologie de mise en place d'une politique de sécurité des systèmes d'information.

Connaissances préalables recommandées (*descriptif succinct des connaissances requises pour pouvoir suivre cet enseignement – Maximum 2 lignes).*

Contenu de la matière :

- Gestion du risque informatique
  - Introduction « Normalisation & SSIC » – ISO/IEC JTC1/SC27
  - Introduction aux aspects méthodologiques de la sécurité
  - PSSI et rôle du RSSI
  - Introduction aux concepts de gestion des risques selon la série ISO/IEC 2700x
  - Le processus de gestion des risques selon la norme ISO/IEC 27005
- Méthodologie pour l'implémentation d'une PSSI
  - Introduction à la méthode EBIOS
  - Implémentation d'une PSSI avec l'ISO/IEC 27002
  - Accréditation, Certification & SSIC
  - La certification ISO/IEC 27001

Mode d'évaluation : *(2 × note examen final + note contrôle continu) / 3*

Références (*Livres et polycopiés, sites internet, etc.).*

- Laurent Bloch, Christophe Wolfhugel, Nat Makarévitch, Christian Queinnec, Hervé Schauer. *Sécurité informatique : Principes et méthodes à l'usage des DSI, RSSI et administrateurs*. Eyrolles, 4ème édition, 2013.
- Alan Calder. Information Security based on ISO 27001/ISO 27002: A Management Guide. Van Haren Publishing, 2ème edition, 2009.

Intitulé du Master : Sécurité des systèmes d'information

Semestre *:* 3
Intitulé de l'UE : UEM3
Intitulé de la matière : Méthodologie avancée de la sécurité
Crédits : 4
Coefficients :2

Objectifs de l'enseignement (*Décrire ce que l'étudiant est censé avoir acquis comme compétences après le succès à cette matière – maximum 3 lignes).*

Aborder le problème de la sécurité dans des infrastructures particulières telles que le cloud.

Connaissances préalables recommandées (*descriptif succinct des connaissances requises pour pouvoir suivre cet enseignement – Maximum 2 lignes).*

Contenu de la matière :

- Sécurité et infrastructures particulières
  - Compléments sur les infrastructures informatiques et leur sécurité
  - Cloud computing, Virtualisation, Media sociaux et Web 2.0
  - Etudes de cas
- Traitement des incidents
  - La gestion quotidienne de la sécurité
  - Réactivité et gestion des incidents selon les contextes : Outsourcing, insourcing, co-sourcing
  - Analyse post-mortem
  - Résilience (DRP, BCP)
  - Etudes de cas

Mode d'évaluation : *(2 × note examen final + note contrôle continu) / 3*

Références *(Livres et polycopiés, sites internet, etc).*

- Tim Mather, Subra Kumaraswamy, Shahed Latif. *Cloud Security and Privacy: An Enterprise Perspective on Risks and Compliance*. O'Reilly Media, 2009.
- Laurent Bloch, Christophe Wolfhugel, Nat Makarévitch, Christian Queinnec, Hervé Schauer. *Sécurité informatique : Principes et méthodes à l'usage des DSI, RSSI et administrateurs*. Eyrolles, 4ème édition, 2013.

Intitulé du Master : Sécurité des systèmes d'information

Semestre *:* 3
Intitulé de l'UE : UEF3
Intitulé de la matière : Sécurité des systèmes d'information
Crédits : 6
Coefficients :3

Objectifs de l'enseignement (*Décrire ce que l'étudiant est censé avoir acquis comme compétences après le succès à cette matière – maximum 3 lignes).*

Etudier les modèles de contrôle d'accès, l'administration avancée, et la protection de données.

Connaissances préalables recommandées (*descriptif succinct des connaissances requises pour pouvoir suivre cet enseignement – Maximum 2 lignes).*

Contenu de la matière :

- Théorie du contrôle d'accès
  - Modèle DAC
  - Modèle MAC
- Administration avancée systèmes
  - Sécurité/ Insécurité des systèmes de l'installation par défaut au système fortifié
  - Sécurité/ Insécurité des réseaux (impacts sur les systèmes des configurations réseaux courantes)
  - Détections des anomalies et des comportements à risques à la volée, entre alerte immédiate et auto-défense d'un système.
- Sécurité des systèmes
  - Définir l'hostilité d'un milieu et adapter son système en conséquence
  - Identification et authentification dans un système, du compte local à l'annuaire de service
  - Les malwares (virus, vers, cheveux de Troie)
  - Les protections des données (RAID, Sauvegarde, Archivage)
  - Les protections des données mobiles (chiffrage)

Mode d'évaluation : *(2 × note examen final + note contrôle continu) / 3*

Références *(Livres et polycopiés, sites internet, etc).*

- David Kim, Michael G. Solomon. *Fundamentals Of Information Systems Security*. Jones & Bartlett Learning, 2ème édition 2013.
- Laurent Bloch, Christophe Wolfhugel, Nat Makarévitch, Christian Queinnec, Hervé Schauer. *Sécurité informatique : Principes et méthodes à l'usage des DSI, RSSI et administrateurs*. Eyrolles, 4ème édition, 2013.

Intitulé du Master : Sécurité des systèmes d'information

Semestre *:* 3
Intitulé de l'UE : UEF3
Intitulé de la matière : Sécurité des réseaux
Crédits : 6
Coefficients :3

Objectifs de l'enseignement (*Décrire ce que l'étudiant est censé avoir acquis comme compétences après le succès à cette matière – maximum 3 lignes).*

Passer en revue l'ensemble des attaques et menaces sur un réseau et former les étudiants aux différentes techniques de protection et de détection d'attaques.

Connaissances préalables recommandées (*descriptif succinct des connaissances requises pour pouvoir suivre cet enseignement – Maximum 2 lignes).*

Contenu de la matière :

- Etude service par service des menaces et attaques (usurpation d'identité, collecte d'informations, déni de services, …)
- Etude détaillée des protections et contre-mesures dans les différentes couches de communication : pare-feu, réseaux privés virtuels, …
- Formation aux mécanismes de détection d'attaques : pots de miels, algorithmes de monitorage de trafic au niveau flux, au niveau paquet, leur modélisation, leur évaluation et leur mise en œuvre
- Etudes de cas sur des traces d'attaques réelles

Mode d'évaluation : *(2 × note examen final + note contrôle continu) / 3*

Références *(Livres et polycopiés, sites internet, etc).*

- Richard Bejtlich. *The Practice of Network Security Monitoring: Understanding Incident Detection and Response.* No Starch Press, 2013.
- Solange Ghernaouti. *Sécurité informatique et réseaux*. Dunod, 4ème édition, 2013.

Intitulé du Master : Sécurité des systèmes d'information

Semestre *:* 3
Intitulé de l'UE : UEF3
Intitulé de la matière : Sécurité des bases de données
Crédits : 6
Coefficients :3

Objectifs de l'enseignement (*Décrire ce que l'étudiant est censé avoir acquis comme compétences après le succès à cette matière – maximum 3 lignes).*

Développer des notions avancées sur les bases de données et présenter les politiques de sécurité relatives aux BD.

Connaissances préalables recommandées (*descriptif succinct des connaissances requises pour pouvoir suivre cet enseignement – Maximum 2 lignes).*

Contenu de la matière :

- Bases de données avancées
  - Bases de données répartie et distribuées, conception et mise en œuvre
  - La logique et les bases de données, requêtes complexes et bases de données déductives
  - Intégrité des données et bases de données actives
- Sécurité des bases de données
  - Politiques de Sécurité relatives aux bases de données, Méthodes d'authentification, Autorisations : privilèges et rôles
  - Mécanismes internes d'audit, Gestion des comptes utilisateurs, Mise en place de contrôles d'accès (triggers)
  - Bases de données Privées Virtuelles
  - Options Avancées de Sécurité

Mode d'évaluation : *(2 × note examen final + note contrôle continu) / 3*

Références *(Livres et polycopiés, sites internet, etc).*

- Ron Ben Natan. *Implementing Database Security and Auditing*. Digital Press, 2005.
- Alfred Basta, Melissa Zgola. *Database Security*. Cengage Learning, 2011.
- Hassan A. Afyouni. *Database Security and Auditing: Protecting Data Integrity and Accessibility*. Cengage Learning, 2005.

Intitulé du Master : Sécurité des systèmes d'information

Semestre *:* 3
Intitulé de l'UE : UEM3
Intitulé de la matière : Techniques de gestion des identités
Crédits : 1
Coefficients :1

Objectifs de l'enseignement (*Décrire ce que l'étudiant est censé avoir acquis comme compétences après le succès à cette matière – maximum 3 lignes).*

Présenter les différentes méthodes et technologies de gestion des identités.

Connaissances préalables recommandées (*descriptif succinct des connaissances requises pour pouvoir suivre cet enseignement – Maximum 2 lignes).*

Contenu de la matière :

- Rappels et compléments sur la gestion des identités
- Solutions technologiques
  - Les smartcard
  - Les lecteurs d'empreinte
  - Les tokens
  - Autres solutions techniques

Mode d'évaluation : *(2 × note examen final + note contrôle continu) / 3*

Références *(Livres et polycopiés, sites internet, etc).*

- Thomas L. Norman. *Electronic Access Control*. Butterworth-Heinemann, 2011.
- Bruno Vincent, Nicolas Debaes, Pierre Pezziardi. *Gestion des Identités : Une Politique pour le Système d'Information*. Octo Technology, 2007.

Intitulé du Master : Sécurité des systèmes d'information

Semestre *:* 3
Intitulé de l'UE : UET3
Intitulé de la matière : Gestion de projet
Crédits : 1
Coefficients :1

Objectifs de l'enseignement (*Décrire ce que l'étudiant est censé avoir acquis comme compétences après le succès à cette matière – maximum 3 lignes).*

Fournir aux étudiants les bases de la conception et de la mise en place d'un projet.

Connaissances préalables recommandées (*descriptif succinct des connaissances requises pour pouvoir suivre cet enseignement – Maximum 2 lignes).*
L'étudiant doit connaitre les étapes d'un projet informatique et maitriser des méthodes de développement d'applications informatiques

Contenu de la matière :

Chapitre 1 : Notions fondamentales

Chapitre 2 : Avant-projet

Chapitre 3 : Planification du projet

Chapitre 4 : Estimation des charges, délais et coûts.

Chapitre 5 : Gestion des Ressources

Chapitre 6 : Mesure et contrôle de l'état d'avancement

Chapitre 7 : Clôture du projet

Mode d'évaluation : *(2 × note examen final + note contrôle continu) / 3*

Références :

· Englender, O., & Fernandes, S. (2012). Manager un projet informatique (3e édition). Eyrolles.

· Gabay, J. (2019). Maîtrise d'ouvrage des projets informatiques : la responsabilité métier tournée vers l'agilité (4e édition, Ser. Infopro. management des systèmes d'information). Dunod.

· Murray, A. (2016). The complete software project manager : mastering technology from planning to launch and beyond. Wiley.

· Stellman, A, ; Greene, J. (2008). Applied software project management, O'Reilly.

V – Curriculum Vitae des Coordonateurs

Curriculum Vitae

Nom et Prénom : Fareh Messaouda

Dernier Diplôme et date d'obtention : Doctorat (Informatique), 2014

Spécialité : Informatique

Grade : MCA

Fonction : Enseignant Chercheur

Etablissement de rattachement : Université de Blida 1, Faculté des Sciences, Département d'Informatique

Publications (pour les 05 dernières années) :

- **Fareh**, M. (2019). Modeling Incomplete Knowledge of Semantic Web Using Bayesian Networks. Applied Artificial Intelligence, 33(11), 1022-1034. DOI: 10.1080/08839514.2019.1661578

- Riali, I., **Fareh**, M., Bouarfa, H. (2019). Fuzzy Probabilistic Ontology Approach: A Hybrid Model for Handling Uncertain Knowledge in Ontologies. International Journal on Semantic Web and Information Systems (IJSWIS), 15(4), 1-20.DOI:10.4018/IJSWIS.2019100101

- Ali Khoudja, M., **Fareh**, M., &; Bouarfa, H. (2022). Deep Embedding Learning With Auto- Encoder for Large-Scale Ontology Matching. International Journal on Semantic Web and Information Systems (IJSWIS), 18(1), 1-18.

- Ali Khoudja M., **Fareh** M.,&; Bouarfa H. (2018), Ontology Matching using Neural Networks: Survey and Analysis, International Conference on Applied Smart Systems (ICASS'2018), 24-25 November 2018, Medea, Algeria.

- Ali Khoudja M., **Fareh** M.,; Bouarfa H. (2018) A New Supervised Learning Based Ontology Matching Approach Using Neural Networks., EMENA-ISTL 2018. (pp.542-551) Morocco.

- Riali, I., **Fareh**, M., Bouarfa, H., (2019). A semantic approach for Handling Probabilistic knowledge of Fuzzy Ontologies. The 21th International Conference on Enterprise Information Systems (ICEIS), Greece. Volume 1, 407-414.

- Hamel, O.,; **Fareh**, M. (2022, September). Encoder-Decoder Neural Network with Attention Mechanism for Types Detection in Linked Data. In 2022 17th Conference on Computer Science and Intelligence Systems (FedCSIS) (pp. 733-739). IEEE.

Modules enseignés :

- Bureautique et technologies web (cours, 1ère année ST),
- Algorithmique1et 2 (cours et TD, 1ère année ST),
- Algorithmique1 et 2 (cours et TD, 2ème année Licence L2),
- Programmation C (cours, TD et TP, 1ère année ST et 2ème année Licence L2),
- Programmation Delphi (TP, 2ème année DEUA),
- Système d'exploitation1 (TD, 3ème année DEUA),
- Fichier (TD, 2ème année DEUA)
- Data Mining (cours et TD, 1ère année Master Ingénierie des logiciels (IL))
- Ingénieries des connaissances et ontologies (cours, 2ème année Master IL),
- Génie Logiciel (TD, 2ème année licence L2),
- Logique Mathématique (TD, 2ème année licence L2),
- Gestion de l'incertain (cours et TD, 2ème année Master SIR),
- Bibliographie (cours, 2ème année Master IL),
- Rédaction scientifique (cours, 2ème année licence L3-SIQ et ISIL)

C U R R I C U L U M V I T A E

First Name: HAFIDA

Last Name: BOUARFA

Date of birthday: 27.12.1965

Familial Situation: Married, 2 children

Title: Professor

Profession: Professor at the Data Processing Department, University of Blida, Algeria

Electronic Address: Hafi.bouarfa@gmail.com hafidabouarfa@hotmail.com**;**

Phone Number: 0555184221

Address: Résidence Chréa, TRB4, Number 37, Blida, ALGERIA

E D U C A T I O N A L H I S T O R Y:

- **Nov. 2004:** PHD in Data Processing, option Information Systems, prepared at the ESI (ex.INI) Algiers, Algeria
- **Dec 1991:** Magister in Data Processing, option Information systems, prepared at the H.E.C of Montréal (Canada).
- **Sep 1988**: Engineer diploma, Data Processing, option information systems, prepared at the ESI (ex. INI) Algiers, Algeria
- **June 1983**: General Certificate of Education, option Mathematics, Algiers, Algeria.

P U B L I C A T I O N S A N D R E S E A R C H W O R K S:

- M. Bersali, A. Rachedi, H. Bouarfa « A New Collaborative Clustering Approach for the Internet of Vehicles (CCA-IoV), Second international conference on Embedded & Distributed Systems, EDIS'2020, 12-13 April. 2020, Oran, Algeria.
- M. Ali Khodja, M. Fareh, H. Bouarfa “Ontology Matching Using Neural Networks: Evaluation for OAEI Tracks”, 6th International Symposium on Modeling and Implementation of Complex Systems”, MISC 2020, 24-26 October, Batna, Algeria.
- F. Zarrouki, S. Ouchani, H. Bouarfa “Towards an Automatic Evaluation of the Performance of Electronic-based Physical Unclonable Functions », 4th International Conference on Artificial Intelligence in Renewable Energetic Systems, IC-AIRES 2020, 22-24 December 2020, Tipaza, Algeria.

- F. Zarrouki, S. Ouchani, H. Bouarfa “Quantifying Security and Performance of Physical Unclonable Functions”, Symposium on Solutions for Smart Cities Challenges 2020, SSCC 2020, December 14-16, 2020, Paris, France.

- F. Zerrouki, S. Ouchani and H. Bouarfa, "Quantifying Security and Performance of Physical Unclonable Functions," 2020 7th International Conference on Internet of Things: Systems, Management and Security (IOTSMS), Paris, France, 2020, pp. 1-4, doi: 10.1109/IOTSMS52051.2020.9340212.

- M. Bersali, A. Rachedi and H. Bouarfa, "A New Collaborative Clustering Approach for the Internet of Vehicles (CCA-IoV)," 2020 Second International Conference on Embedded & Distributed Systems (EDiS), Oran, Algeria, 2020, pp. 58-63, doi: 10.1109/EDiS49545.2020.9296436.

- F. Zerrouki, S.Ouchani, H. Bouarfa, “A survey on silicon PUFs”, Journal of Systems Architecture, Volume 127, 2022

- W.D. Miloud, S. Ouchani, H. Bouarfa, “Towards a reliable smart city through formal verification and network analysis”, Computer Communications, Volume 180, 2021

- F. Zerrouki, S. Ouchani, H. Bouarfa, “Towards a Foundation of a Mutual Authentication Protocol for a Robust and Resilient PUF-Based Communication Network”, Procedia Computer Science, Volume 191, 2021

- F. Zerrouki, S. Ouchani, H. Bouarfa, “A Low-Cost Authentication Protocol Using Arbiter-PUF”. In: Attiogbé, C., Ben Yahia, S. (eds) Model and Data Engineering. MEDI 2021. Lecture Notes in Computer Science, vol 12732. Springer, Cham. https://doi.org/10.1007/978-3-030-78428-7_9

- F. Zerrouki, S. Ouchani, H. Bouarfa, H. “A Generation and Recovery Framework for Silicon PUFs Based Cryptographic Key”. In: Bellatreche, L., Chernishev, G., Corral, A., Ouchani, S., Vain, J. (eds) Advances in Model and Data Engineering in the Digitalization Era. MEDI 2021. Communications in Computer and Information Science, vol 1481. Springer, Cham. https://doi.org/10.1007/978-3-030-87657-9_10

- F. Zerrouki, S. Ouchani, H. Bouarfa, “Towards an Automatic Evaluation of the Performance of Physical Unclonable Functions”. In: Hatti, M. (eds) Artificial Intelligence and Renewables Towards an Energy Transition. ICAIRES 2020. Lecture Notes in Networks and Systems, vol 174. Springer, Cham. https://doi.org/10.1007/978-3-030-63846-7_74

- M. Bersali, A. Rachedi and H. Bouarfa, "Convolutional neural network for relays selection in the Internet of Vehicles," 2021 International Conference on Forthcoming Networks and Sustainability in AIoT Era (FoNeS-AIoT), Nicosia, Turkey, 2021, pp. 57-61, doi: 10.1109/FoNeS-AIoT54873.2021.00022.

- W.D. Miloud, S. Ouchani, H. Bouarfa “Guaranteeing Information Integrity Through Blockchains for Smart Cities”. In: Attiogbé, C., Ben Yahia, S. (eds) Model and Data Engineering. MEDI 2021. Lecture Notes in Computer Science, vol 12732. Springer, Cham. https://doi.org/10.1007/978-3-030-78428-7_16

- M. Bersali, A. Rachedi and H. Bouarfa “A novel cooperative clustering approach based on multi-criteria decision-making for IoV”, International Journal of High-Performance Systems Architecture, Vol 11(1), 2022.

- Ali Khoudja, M., M. Fareh, and H. Bouarfa, Deep Embedding Learning With AutoEncoder for Large-Scale Ontology Matching. International Journal on Semantic Web and Information Systems (IJSWIS), 2022. 18(1): p. 1-18.

- Z. Diffallah, H. Ykhlef, H. Bouarfa and N. Diffallah, "Consistency Regularization-Based Polyphonic Audio Event Detection with Minimal Supervision," 2022 IEEE 21st international Conference on Sciences and Techniques of Automatic Control and Computer Engineering (STA), Sousse, Tunisia, 19-21 dec; 2022, pp. 325-330, doi: 10.1109/STA56120.2022.10019247.

- M. Aiche, S. Ouchani, H, Bouarfa, “Leader-Assisted Client Selection for Federated Learning in IoT via the Cooperation of Nearby Devices”, In: Renault, É., Mühlethaler, P. (eds) Machine Learning for Networking. MLN 2022. Lecture Notes in Computer Science, vol 13767. Springer, Cham. https://doi.org/10.1007/978-3-031-36183-8_12

- Z. Diffallah, H. Ykhlef and H. Bouarfa, "Mean Teacher for Weakly Supervised Polyphonic Sound Event Detection: An Empirical Study," 2022 7th International Conference on Image and Signal Processing and their Applications (ISPA), Mostaganem, Algeria, 8-9 Mai 2022, pp. 1-6, doi: 10.1109/ISPA54004.2022.9786322.

- W.D. Miloud., S. Ouchani, H. Bouarfa “Guaranteeing information integrity and access control in smart cities through blockchain”, J Ambient Intell Human Comput 14, 11419–11428 (2023). https://doi.org/10.1007/s12652-022-03718-y

- F. Zerrouki, S. Ouchani, H. Bouarfa, “PUF-based mutual authentication and session key establishment protocol for IoT devices”, J Ambient Intell Human Comput 14, 12575–12593 (2023). https://doi.org/10.1007/s12652-022-04321-x

- F. Zerrouki, S. Ouchani, H. Bouarfa, “T2S-MAKEP and T2T-MAKEP: A PUF-based Mutual Authentication and Key Exchange Protocol for IoT devices”, Internet of Things, Elsevier, 2023.

Comité Scientifique de département

Avis et visa du Comité Scientifique : Favorable

Date : 25/02/2024

رئيس اللجنة العلمية لقسم الاعلام الالي

Conseil Scientifique de la Faculté (ou de l'institut)

Avis et visa du Conseil Scientifique :

Favorable

Date : 25/02/2024

Présidente du Conseil Scientifique
de la Faculté des Sciences
Pr. A B E D Hafida

Doyen de la faculté (ou Directeur d'institut)

Avis et visa du Doyen ou du Directeur :

Date :

Conseil Scientifique de l'Université (ou du Centre Universitaire)

Avis et visa du Conseil Scientifique :

Date :

VIII - Visa de la Conférence Régionale

(Uniquement à renseigner dans la **version finale** de l'offre de formation)

.