UNIVERSITÉ TOULOUSE III PAUL SABATIER

Université de Toulouse

Faculté Sciences et Ingénierie

PÉRIODE D'ACCRÉDITATION : 2016 / 2021

UNIVERSITÉ PAUL SABATIER

SYLLABUS MASTER

Mention Réseaux et Télécommunication

M2 sécurité des systèmes d'information et des réseaux

http://www.fsi.univ-tlse3.fr/

2018 / 2019

24 FÉVRIER 2019

SOMMAIRE

PRÉSENTATION

PRÉSENTATION DU PARCOURS

PARCOURS

La formation est totalement dédiée à la problématique de la sécurité et à la sûreté des systèmes d'information conduisant à un haut niveau d'expertise en sécurité des réseaux, des systèmes et des applications. Le diplômé acquiert les compétences lui permettant de garantir la sécurité applicative avec assurance et autorité tout en facilitant le succès du dialogue métier. La formation vise les débouchés relatifs à la mise en œuvre de politiques et de dispositifs de sécurité en déployant les outils et les processus de prévention, de diagnostic et de remédiation.

PRÉSENTATION DE L'ANNÉE DE M2 SÉCURITÉ DES SYSTÈMES D'INFORMATION ET DES RÉSEAUX

Les systèmes d'information étant de plus en plus complexes et face à la cybercriminalité, la sécurité des applications et des données devient une préoccupation majeure des entreprises, voire un enjeu stratégique. L'expert en sécurité informatique est recherché par les donneurs d'ordre, les entreprises de service numérique (ESN), les prestataires spécialisés en sécurité informatique. Les secteurs d'activité recouvrent largement ceux de l'industrie, le secteur bancaire et financier, la santé et les biotechnologies, les nouvelles technologies de l'information et de la communication.
La certification atteste du haut niveau d'expertise du futur collaborateur et de sa constante adaptabilité aux évolutions de son environnement organisationnel et technologique.
L'expert en sécurité informatique met en œuvre la sécurité et la sûreté des systèmes et des applications. Il évalue la vulnérabilité des systèmes et met en place des solutions pour protéger les applications et les données. Il intervient par des procédures de niveaux technique, méthodologique et organisationnel.
Support technique sur les projets, il travaille en étroite collaboration avec les équipes techniques, les responsables d'architecture système et les services métiers. Il est en contact régulier avec les RSSI ou leurs représentants. Il doit comprendre les besoins des projets et apporte son expertise sécurité à toutes les étapes de développement des architectures matérielles et logicielles des projets informatiques : la définition, la planification et le déploiement ou la migration de nouvelles infrastructures.
Au quotidien, il définit, implémente et contrôle les exigences de sécurité permettant de garantir le niveau de protection des systèmes d'informations de son périmètre tout en respectant les contraintes de sûreté de fonctionnement.
Il sait auditer le système d'information et investiguer de bout en bout les infrastructures réseau, système et applicative sous l'angle sécurité. Il peut prescrire les recommandations au traitement des problèmes techniques.
En complément, il maitrise les différentes normes de sécurité organisationnelles et techniques s'appliquant aux différents domaines métiers.
Il rédige les rapports d'analyse et de préconisations ainsi que les plans d'action et d'amélioration techniques et organisationnels.
Il se tient informé sur l'évolution des normes et procédures de sécurité ainsi que sur les outils et les technologies s'y rapportant. Il assure une veille sur les aspects juridiques en matière de sécurité et de droit informatique.
La formation en dernière année est organisée en alternance. Une première période de mi-septembre à mi-janvier en continu à l'université est entrecoupée par une immersion en entreprise de 3 semaines à la mi-octobre. Suit une deuxième période en alternance jusqu'à mi-septembre à raison d'un jour par semaine de formation en dehors des périodes de vacances scolaires.

RUBRIQUE CONTACTS

CONTACTS PARCOURS

RESPONSABLE M2 SÉCURITÉ DES SYSTÈMES D'INFORMATION ET DES RÉSEAUX

BENZEKRI Abdelmalek
Email : benzekri@irit.fr

SECRÉTAIRE PÉDAGOGIQUE

ROQUES Geraldine
Email : geraldine.roques@univ-tlse3.fr

CONTACTS MENTION

RESPONSABLE DE MENTION RÉSEAUX ET TÉLÉCOMMUNICATION

AOUN André
Email : Andre.Aoun@irit.fr

CONTACTS DÉPARTEMENT: FSI.INFO

DIRECTEUR DU DÉPARTEMENT

CROUZIL Alain
Email : Téléphone : 05 61 55 69 28

SECRETARIAT DU DÉPARTEMENT

LESTRADE Colette
Email : Téléphone : 05 61 55 81 58

Université Paul Sabalier
1TP1-14
118 route de Narbonne
31062 TOULOUSE cedex 9

TABLEAU SYNTHÉTIQUE DES UE DE LA FORMATION

page	Code	Intitulé UE	ECTS	Obligatoire Facultatif	Cours	TD	Projet	Stage
Premier semestre								
8	EIRTB3AM	SÉCURITÉ DES RÉSEAUX DE COMMUNICATION	5	O	15	45		
9	EIRTB3BM	SÉCURITÉ APPLICATIVE	6	O	20	55		
10	EIRTB3CM	SÉCURITÉ ET SÛRETÉ	4	O	12	33		
11	EIRTB3DM	ÉCOSYSTÈME, GOUVERNANCE ET ASPECTS OPÉRATIONNELS DE LA SÉCURITÉ	9	O	25	50	50	
12	EIRTB3EM	COMMUNICATION	3	O		30		
13	EIRTB3VM	ANGLAIS	3	O		24		
Second semestre								
14	EIRTB4AM	SÉCURITÉ DES SYSTÈMES ET DES COMPOSANTS	5	O	16	44		
15	EIRTB4BM	GESTION DES IDENTITÉS ET DES ACCÈS	3	O	10	20		
16	EIRTB4CM	ASPECTS JURIDIQUES ET TESTS INTRUSIFS ET FORENSIC	4	O	17	28		
17	EIRTB4DM	STAGE	18	O				4

LISTE DES UE

UE	SÉCURITÉ DES RÉSEAUX DE COMMUNICATION	5 ECTS	1er semestre
EIRTB3AM	Cours : 15h , TD : 45h		

ENSEIGNANT(E) RESPONSABLE

BENZEKRI Abdelmalek
Email : benzekri@irit.fr

OBJECTIFS D'APPRENTISSAGE

Ce cours présente les vulnérabilités des protocoles et réseaux de communication filaires et non filaires. Les techniques et outils constituant les mécanismes de sécurité sont étudiés en détail et leur mise en oeuvre est appliquée aux réseaux TCP/IP.
La conception d'architectures de réseaux robustes et sécurisés est également traitée et des solutions sont évaluées : analyse de trafic, sondes, systèmes de prévention et/ou de détection d'intrusion, relais et tunnels VPNs.
La configuration et l'administration de solutions sont mises en pratiques dans des environnements Linux et ASA CIsco.

DESCRIPTION SYNTHÉTIQUE DES ENSEIGNEMENTS

- vulnérabilités des protocoles de communication (typologie des attaques contre les réseseaux filaires et sans fil)- techniques de chiffremement asymétrique/symétrique/hybride, codes d'authentification de message- mécanismes de sécurité pour les protocoles de communication- outils et techniques pour la sécurité (chiffrement, translation adresses, ports, contrôle d'admission et d'utilisation de ressources (listes de contrôle d'accès...), Snort)- sécurisation des accès réseaux et serveurs dans un réseau local (construction de pare feux, mise en œuvre de VLAN, mise en place de proxys, protocoles réseaux sécurisés (IPsec))- sécurisation des accès réseaux à distance (solution opérateurs (tunnels, accès distants), analyse de trafic réseau, VPN, pare-feu, IDS)- sécurisation des solutions non filaires (WiFi - Réseaux cellulaires)- architecture de passerelle sécurisée- protocoles de tunnelisation (PPTP, L2TP, IPsec, SSL/TLS, SSH)- administration réseau et sécurité (configuration, sondes, scans, audits, journaux)- AAA : protocoles d'authentification utilisateurs/adresses - Radius, 802.1x, EAP et extensions, PKI- manipulation de matériel ASA Cisco dédié- Virtualisation de réseaux

PRÉ-REQUIS

Concepts fondamentaux des réseaux informatiques - Réseaux TCP/IP - Protocoles TCP/IP

MOTS-CLÉS

TCP/IP - Firewall - IDS/IPS - VPN - Ipsec - SSH - SSL/TLS - architecture de passerelle sécurisée

UE	SÉCURITÉ APPLICATIVE	6 ECTS	1^{er} semestre
EIRTB3BM	Cours : 20h , TD : 55h		

ENSEIGNANT(E) RESPONSABLE

BENZEKRI Abdelmalek
Email : benzekri@irit.fr

OBJECTIFS D'APPRENTISSAGE

Les principales vulnérabilités des applications réseau sont recensées. La sécurité des applications majeures de l'Internet (DNSSEC, messagerie, web sécurisé et téléphonie) est rappelée.
L'étude des problèmes de sécurité dans un contexte de développement d'applications et de systèmes informatiques sécurisés est considérée dans toutes les phases de développement (analyse - exigences, architecture, codage, test, intégration, déploiement, exploitation et maintenance). Les méthodes d'ingénierie logicielles SDL de Microsoft et CLAP d'OWASP sont présentées.
Les vulnérabilités logicielles connues sont analysées et des contre-mesures présentées en particulier autour du langage C.
La rétroingénierie de logiciels est traitée. Des contre-mesures sont présentées pour rendre cette activité plus difficile.

DESCRIPTION SYNTHÉTIQUE DES ENSEIGNEMENTS

- DNSSEC - messagerie électeonique (SMIME) - sécurisation Web - Firewalls applicatifs
- Identification des vulnérabilités par analyse statique de code(débordement dans la pile, "return into libc", débordement dans le tas) - Contre-mesures techniques (mécanismes de protection usuels des compilateurs, technique du canari, distribution aléatoire de l'espace d'adressage (ASLR), etc.)
- Reverse engineering : méthodologie et outils - désassembleurs, débuggers et languages de scripting -
- Sécurité des Applications Web : Sécurité dans le navigateur - techniques d'attaques - techniques de protection - Sécurité du réseau - Sécurité dans le serveur applicatif (modèle MVC - contrôle d'accès - sécurité dans le cloud : virtualisation et modèles de sécurité)
- Revue de code - Fuzzing
- Ingénierie de développement sécurisé (SDL de Microsoft, CLAP OWASP)

Sécurité des données - Architecture logicielle type d'un SGBD relationnel - Architectures n-tiers applicatives - Contrôle des droits d'accès - Vues relationnelles et confidentialité - Intégrité et cohérence des données -
Injection de code SQL et par canaux d'inférence - défense : procédures stockées, contrôle d'inférence et chiffrement des données

UE	SÉCURITÉ ET SÛRETÉ	4 ECTS	1^{er} semestre
EIRTB3CM	Cours : 12h , TD : 33h		

ENSEIGNANT(E) RESPONSABLE

BENZEKRI Abdelmalek
Email : benzekri@irit.fr

OBJECTIFS D'APPRENTISSAGE

Ce cours introduit la problématique de sûreté de fonctionnement, présente des solutions d'architecture et inventorie les mécanismes de tolérance aux fautes. La coordination/coopération entre le logiciel et le matériel est étudiée pour assurer la protection contre les attaques internes (sûreté de fonctionnement) et externes (sécurité).Les techniques d'évaluation qualitative et quantitative et de prévision des fautes sont également traitées. Un tour d'horizon des normes de sûreté et des niveaux d'assurance permet d'introduire la sûreté du logiciel à travers l'utilisation des méthodes formelles (expression, vérification et preuve de propriétés).

DESCRIPTION SYNTHÉTIQUE DES ENSEIGNEMENTS

- introduction et concepts de base (enjeux, définitions de base : attributs, entraves, moyens) techniques pour la tolérance aux fautes (hypothèses de fautes, techniques de base pour la détection et le recouvrement d'erreurs)
- stratégies de réplication (solutions architecturales et exemples)
- vérification et test (analyse statique, model checking et preuves formelles - techniques de test du logiciel)
- évaluation de la sureté de fonctionnement (mesures, évaluation à base de modèles, approches expérimentales, fiabilité du logiciel)

UE	ÉCOSYSTÈME, GOUVERNANCE ET ASPECTS OPÉRATIONNELS DE LA SÉCURITÉ	9 ECTS	1er semestre
EIRTB3DM	Cours : 25h , TD : 50h , Projet : 50h		

ENSEIGNANT(E) RESPONSABLE

BENZEKRI Abdelmalek
Email : benzekri@irit.fr

OBJECTIFS D'APPRENTISSAGE

Reconnaître les acteurs chargés de la sécurité à l'intérieur et autour d'une entreprise.
Identifier les enjeux et les parties prenantes, au sein d'une organisation, pour définir et esquisser une démarche de gouvernance de la sécurité.
Présenter l'organisation et la gestion de la sécurité des systèmes d'information, la conduite d'audits organisationnels et techniques pour l'évaluation de la sécurité. Les méthodologies d'analyse des risques sont considérées avec un intérêt particulier pour la méthode EBIOS. Sont traitées également les politiques de sécurité permettant d'intégrer et de déployer les mesures de sécurité en réponse à l'analyse de risques. Une veille des bonnes pratiques en matière de sécurité des SI clôt le tour d'horizon organisationnel de la sécurité des SI.

DESCRIPTION SYNTHÉTIQUE DES ENSEIGNEMENTS

- enjeux de la sécurité des systèmes d'information - Sites de veille - Inventaire des acteurs et de leurs apports en regard de la SSI (rôle et organismes (ANSSI, FIRST, CERT, CLUSIF, 27001, ITSMF), normalisation, sécurité et bonnes pratiques (série ISO 27000, ISO 15408, ISO 13335, ISO 7498, ITIL)- ANSSI : Référentiel général de la sécurité RGS - qualification de produits de sécurité - qualification de prestataires - référentels d'exigences - - Modèles de sécurité - Contrôles et mesures de sécurité - gestion de la sécurité de l'information (ISO 27001) - mise en place d'un SMSI - accompagnement au changement- Gestion des risques en sécurité de l'information - Méthode EBIOS- Evaluation de la sécurité - techniques d'audit - ISO 19001 - Principes d'audit - Conduite d'audit de certification - Politiques de sécurité et chartes - Retour d'expérience ISO 27001 : de la décision à la certification- Sécurité opérationnelle : Méthode et Outils SIEM - mise en place d'un SOC

UE	COMMUNICATION	3 ECTS	1er semestre
EIRTB3EM	TD : 30h		

UE	ANGLAIS	3 ECTS	1^{er} semestre
EIRTB3VM	TD : 24h		

ENSEIGNANT(E) RESPONSABLE

CHAPLIER Claire
Email : claire.chaplier@univ-tlse3.fr

UE	SÉCURITÉ DES SYSTÈMES ET DES COMPOSANTS	5 ECTS	2nd semestre
EIRTB4AM	Cours : 16h , TD : 44h		

ENSEIGNANT(E) RESPONSABLE

BENZEKRI Abdelmalek
Email : benzekri@irit.fr

UE	GESTION DES IDENTITÉS ET DES ACCÈS	3 ECTS	2nd semestre
EIRTB4BM	Cours : 10h , TD : 20h		

ENSEIGNANT(E) RESPONSABLE

BENZEKRI Abdelmalek
Email : benzekri@irit.fr

UE	ASPECTS JURIDIQUES ET TESTS INTRUSIFS ET FORENSIC	4 ECTS	2nd semestre
EIRTB4CM	Cours : 17h , TD : 28h		

ENSEIGNANT(E) RESPONSABLE

BENZEKRI Abdelmalek
Email : benzekri@irit.fr

UE	STAGE	18 ECTS	2nd semestre
EIRTB4DM	Stage : 4 mois minimum		

ENSEIGNANT(E) RESPONSABLE

BENZEKRI Abdelmalek
Email : benzekri@irit.fr

GLOSSAIRE

TERMES GÉNÉRAUX

DÉPARTEMENT

Les départements d'enseignement sont des structures d'animation pédagogique internes aux composantes (ou facultés) qui regroupent les enseignants intervenant dans une ou plusieurs mentions

UE : UNITÉ D'ENSEIGNEMENT

Unité d'Enseignement. Un semestre est découpé en unités d'enseignement qui peuvent être obligatoire, optionnelle (choix à faire) ou facultative (UE en plus). Une UE représente un ensemble cohérent d'enseignements auquel est associé des ECTS.

ECTS : EUROPEAN CREDITS TRANSFER SYSTEM

Les ECTS sont destinés à constituer l'unité de mesure commune des formations universitaires de Licence et de Master dans l'espace européen depuis sa création en 1989. Chaque UE obtenue est ainsi affectée d'un certain nombre d'ECTS (en général 30 par semestre d'enseignement). Le nombre d'ECTS est fonction de la charge globale de travail (CM, TD, TP, etc.) y compris le travail personnel. Le système des ECTS vise à faciliter la mobilité et la reconnaissance des diplômes en Europe.

TERMES ASSOCIÉS AUX DIPLOMES

Les diplômes sont déclinés en domaines, mentions et parcours.

DOMAINE

Le domaine correspond à un ensemble de formations relevant d'un champ disciplinaire ou professionnel commun. La plupart de nos formations relèvent du domaine Sciences, Technologies, Santé.

MENTION

La mention correspond à un champ disciplinaire. Elle comprend, en général, plusieurs parcours.

PARCOURS

Le parcours constitue une spécialisation particulière d'un champ disciplinaire choisie par l'étudiant au cours de son cursus.

TERMES ASSOCIÉS AUX ENSEIGNEMENTS

CM : COURS MAGISTRAL(AUX)

Cours dispensé en général devant un grand nombre d'étudiants (par exemple, une promotion entière), dans de grandes salles ou des amphis. Au-delà de l'importance du nombre d'étudiants, ce qui caractérise le cours magistral, est qu'il est le fait d'un enseignant qui en définit lui-même les structures et les modalités. Même si ses contenus font l'objet de concertations entre l'enseignant, l'équipe pédagogique, chaque cours magistral porte la marque de l'enseignant qui le dispense.

TD : TRAVAUX DIRIGÉS

Ce sont des séances de travail en groupes restreints (de 25 à 40 étudiants selon les composantes), animés par des enseignants. Ils illustrent les cours magistraux et permettent d'approfondir les éléments apportés par ces derniers.

TP : TRAVAUX PRATIQUES

Méthode d'enseignement permettant de mettre en pratique les connaissances théoriques acquises durant les CM et les TD. Généralement, cette mise en pratique se réalise au travers d'expérimentations. En règle générale, les groupes de TP sont constitué des 16 à 20 étudiants. Certains travaux pratiques peuvent être partiellement encadrés voire pas du tout. A contrario, certains TP, du fait de leur dangerosité, sont très encadrés (jusqu'à 1 enseignant pour quatre étudiants).

PROJET OU BUREAU D'ÉTUDE

Le projet est une mise en pratique en autonomie ou en semi-autonomie des connaissances acquises. il permet de vérifier l'acquisition des compétences.

TERRAIN

Le terrain est une mise en pratique encadrée des connaissances acquises en dehors de l'université.

STAGE

Le stage est une mise en pratique encadrée des connaissances acquises dans une entreprise ou un laboratoire de recherche. Il fait l'objet d'une législation très précise impliquant, en particulier, la nécessité d'une convention pour chaque stagiaire entre la structure d'accueil et l'université.


UNIVERSITÉ
TOULOUSE III
PAUL SABATIER
Université
de Toulouse