FORMATION CONTINUE

Master

informatique

sécurité des systèmes d'information

Diplôme national - niveau bac+5 - formation à temps plein

Formation éligible au CPF
Compte Personnel de Formation

Les codes de référence utiles pour solliciter votre CPF sont disponibles sur : sfc.univ-rennes1.fr

Informations et inscriptions

Université de Rennes 1
Service formation continue
6, rue Kléber - CS 16926
35069 Rennes CEDEX
Tél : 02 23 23 39 50
sfc@univ-rennes1.fr

Contacts

Chargé de mission
Guillaume RIOU

Assistante de formation
Mélanie LECRU

Coordination pédagogique

Pierre-Alain FOUQUE
ISTIC

En savoir plus :
sfc.univ-rennes1.fr

Qualification des Services Intellectuels ISQ OPQF
spécialités de formation : 1M 2B

Public

Cette formation s'adresse aux professionnels du secteur informatique qui souhaitent essentiellement développer des compétences en sécurité des systèmes d'information. Un goût pour les technologies ayant trait aux réseaux, mais aussi à l'administration des systèmes d'information est indispensable.
Les professionnels peuvent y trouver aussi la valorisation d'une expérience et de fonctions dans l'entreprise par l'obtention d'un diplôme national.

Objectifs, compétences développées

La spécialité sécurité des systèmes d'information (SSI) permet à des informaticiens de niveau bac+4 de se spécialiser dans le domaine de la sécurité des systèmes informatiques. Les aspects couverts par ce domaine couvrent un spectre très large et il est difficile d'en faire le tour. C'est pourquoi il a été fait le choix de mettre en avant deux thématiques plus particulièrement. Le cursus s'articule donc autour d'un premier axe consacré à la conception de logiciels sûrs (techniques de génie logiciel, mais aussi détournement du fonctionnement des programmes mal conçus), et enfin d'un second axe consacré à la sécurité des réseaux et des systèmes d'exploitation.

Débouchés

Le type de profil des informaticiens formés par cette spécialité SSI intéresse à la fois des grandes entreprises pour lesquelles la fonction d'ingénieur de sécurité fait maintenant partie du vocabulaire courant, mais aussi les PME où les candidats pourront développer une activité polymorphe en prenant en charge l'étude, la conception et la mise en œuvre du système d'information pour lequel ils pourront déployer les connaissances et les technologies acquises lors du cursus.
Les entreprises accueillant les stagiaires du master SSI démontrent par leur réponse la parfaite adéquation de notre formation à leur attente. Lorsque des postes sont ouverts au recrutement, les stagiaires sont employés immédiatement à l'issue de leur stage par leur entreprise d'accueil.

Condition d'accès

Expérience professionnelle de 3 ans minimum en informatique
Diplôme de niveau bac+4 ou moins, mais avec de solides acquis professionnels en informatique (validation des acquis)
Sélection sur dossier et entretien.

Organisation pédagogique

La formation comprend des cours magistraux, des travaux dirigés et des travaux pratiques effectués avec les moyens techniques de l'ISTIC. Pendant toute la durée de la formation,

UNIVERSITÉ DE RENNES 1
FORMATION CONTINUE

MASTER

sécurité des systèmes d'information

Modalités pratiques

Prix de la formation :
- 4 355 € (droits d'inscription universitaire compris)

Durée :
- 6 mois de cours
- 5 à 6 mois de stage pratique en entreprise

Lieu :
- Rennes

Nombre de places :
- 4

Constitution du dossier :
- dossier de candidature.
- 1 photo d'identité
- photocopie des diplômes
- brochure de présentation de l'entreprise.

Calendrier

Date limite de dépôt de dossier :
- mi-mars pour les candidats ne résidant pas en France
- mi-mai pour les autres candidats.

Début des cours :
- fin août

Stage en entreprise :
- de mars à août

Soutenance de mémoire de stage :
- début septembre

les stagiaires bénéficient d'une permanence pédagogique assurée par un enseignant de l'ISTIC, de l'accès à une bibliothèque spécifique ainsi qu'aux salles de travaux pratiques (machines).
La formation théorique est organisée en unités d'enseignement (UE) regroupées par semestres.
La validation se fait par crédits (ECTS). Les UE des enseignements de base (18 ECTS) et des options ou modules libres (12 ECTS) ont lieu au premier semestre et le stage (30 ECTS) au second.
En fonction de son projet professionnel, chaque étudiant choisit trois UE optionnelles parmi celles proposées. Les étudiants de formation continue doivent en plus suivre l'UE libre MNCO.
Un stage en entreprise donne aux participants la possibilité de mettre en pratique les connaissances acquises et de saisir la dimension réelle d'un projet industriel.

Programme

Semestre 1

Méthodologie pour la politique de sécurité (MOPS) (3 ECTS) **:**
- introduction destinée à donner aux étudiants le vocabulaire et la culture nécessaires à une bonne compréhension des politiques de sécurité ;
- méthodologie applicable dans la réalité de l'entreprise, en ce qui concerne la définition d'une politique de sécurité ainsi que sa mise en oeuvre dans la pratique.

Base de la cryptographie pour la sécurité (BCS) (3 ECTS) **:**
- notions de base à propos de la cryptographie et de la cryptanalyse ;
- initiation aux modèles et preuves de sécurité ;
- présentation des schémas classiques de cryptographie à clé symétrique que sont le One-Time Pad et les schémas de chiffrement par flots, les schémas de chiffrement par blocs (DES, AES) et les modes opératoires de chiffrement, les fonctions de hachages et les codes d'authentification de messages.
- présentation des problèmes et schémas de cryptographie à clé publique de signature et de chiffrement comme RSA et El Gamal seront décrit ;
- découverte du protocole d'échange de clé Diffie-Hellman.

Administration des réseaux Internet (ADMI) (3 ECTS) **:**
- comprendre les protocoles qui interviennent dans l'administration des réseaux ;
- maîtriser les outils d'aide à l'administration ;
- savoir organiser les réseaux pour faciliter leur administration.

Génie logiciel appliqué : conception de logiciel sûrs (GLA) (3 ECTS) **:**
- découvrir la programmation en utilisant UML ;
- techniques de test, de prévention des défauts et de correction des fautes détectées (diagnostic et «debugging») ;
- si le temps le permet, le cours présentera aussi des techniques pour écrire du code sécurisé.

Cellule insertion professionnelle

À destination des stagiaires en reprise d'études ou engagés dans un processus de validation d'acquis, nous vous accompagnons dans vos recherches d'emploi ou de stage :
- en vous apportant un service comportant des ateliers, un module de techniques de recherche d'emploi en ligne, un forum d'échange et un accès à nos réseaux sociaux ;
- en sélectionnant des offres, au sein des sites d'emploi en lien avec les formations de l'université de Rennes 1 ;
- en effectuant une revue de presse vous permettant d'aborder le marché caché de l'emploi ;
- en renforçant votre présence au cœur des manifestations d'entreprises.

La cellule IP met également à votre disposition, des enquêtes d'insertion sur les diplômes de l'université de Rennes 1.

MASTER

sécurité des systèmes d'information

Sécurité des réseaux informatiques (SRI) (3 ECTS) **:**

- découvrir les protocoles de sécurisation des réseaux que sont les firewalls, les outils de détection d'intrusion, les protocoles d'authentifications du type Radius, les PKI et les VPN.

Étude des vulnérabilités des logiciels (EVL) (3 ECTS) **:**

- comprendre les vulnérabilités qui peuvent affecter les programmes développés dans des langages où la gestion de la mémoire est effectuée directement par le programmeur (par exemple C, C++, qui constituent une part importante des logiciels disponibles à l'heure actuelle) ;
- s'intéresser aux mécanismes (au niveau du système d'exploitation, du compilateur) permettant de détecter ces vulnérabilités, voire d'en empêcher le déclenchement à l'exécution.

Techniques d'expression (EXP) (5 ECTS) **:**

- communication ;
- culture scientifique ;
- anglais ;
- travail prospectif individuel ;
- projet.

Ce module de base, commun à tous les masters professionnels en informatique.

Option - trois enseignements à choisir en début d'année (6 ETCS) **:**

Les enseignements proposés peuvent varier chaque année en fonction des évolutions technologiques du domaine.

Architecture et technologie des réseaux (ATR) :

- éléments d'ingénierie pour la mise en œuvre d'architectures en prenant en compte les problématiques de sécurité ;
- modèles d'architectures fonctionnelles.

Authentification (AUTH) :

- étude des différentes facettes de l'authentification : Kerberos, authentification dans les réseaux sans fil, authentification par biométrie, accréditation anonymes, sécurité matérielle et authentification.

Contrôle d'accès (CA) :

- présenter l'expression de propriétés de sécurité et la définition de politiques de sécurité selon des modèles de sécurité éprouvés ;
- analyser des modèles formels de contrôle d'accès, de flux et d'usage, dans le cadre des systèmes d'information et des systèmes d'exploitation.

Protection de la vie privée (PVP) :

- présentation d'un panorama des différentes situations du monde numérique qui peuvent conduire à un bris de vie privée ainsi que leurs conséquences ;
- étude des technologies respectueuses de la vie privée ainsi que les principes fondamentaux qui les sous-tendent.

Systèmes de détection d'intrusions (IDS) :

- étude des différentes approches permettant la détection d'intrusions (approche comportementale, approche par connaissance) ;
- mise en oeuvre pratique de tels systèmes et test de leurs efficacités respectives.

sécurité des systèmes d'information

Cryptographie avancée (CRYPT) :

- renforcement du cours BCS en présentant des attaques et en particulier les attaques par canaux auxiliaires, les preuves de sécurité, les schémas à base de courbes elliptiques et d'autres aspects plus pratiques comme les générateurs aléatoires et les produits cryptographiques disponibles sous forme de logiciels libres comme les mécanismes de chiffrement de disques durs ou les logiciels de chiffrement de messages (PGP).

Cartes à puce (CAP) :

- cours commun au master 2 **crypto** : sécurité des cartes à puces.

Libre et obligatoire : mise à niveau en compilation (MNCO) (1 ECTS) :

- techniques de compilation : analyses lexicale, syntaxique, sémantique ;
- génération de code.

Semestre 2

Stage en entreprise (au moins 4 mois - 30 ECTS) :

Stage à temps complet.
La recherche du stage incombe au stagiaire. Le stage est typiquement orienté vers une réalisation pratique (le sujet doit être validé par le responsable de la formation)

Si vous êtes étudiant, veuillez prendre contact avec la scolarité de l'ISTIC
tél. : +33 (0)2 23 23 39 07 - secr-m2-info-pro@univ-rennes1.fr