UNIVERSITÉ DE RENNES 1

Sciences, Technologies, Santé

Master

MENTION INFORMATIQUE

SPÉCIALITÉ

SÉCURITÉ DES SYSTEMES D'INFORMATION

Objectifs de la formation :

Concevoir des logiciels sûrs (techniques de génie logiciels mais aussi analyser des erreurs de conception des programmes)
Sécuriser les réseaux et les systèmes d'exploitation ainsi que les échanges dont ils sont le support.

Choisir les dispositifs techniques de sécurité les plus appropriés aux besoins de l'entreprise.

Domaines de connaissances	Capacités ou savoir-faire associés
Méthodologie pour la politique de sécurité	▪ Analyser les risques spécifiques au secteur ▪ Rédiger une politique de sécurité (normes, indicateurs..) ▪ Mettre en œuvre les mesures qui en découlent
Bases de la cryptographie pour la sécurité	▪ Comprendre les concepts mathématiques sous-jacents à la cryptographie ▪ Analyser des protocoles cryptographiques à l'aide d'outils de vérification formelle
Administration des réseaux informatiques	▪ Faire face aux principaux problèmes liés à l'administration et à la configuration d'un réseau informatique (protocoles de routage, surveillance du réseau, administration de stations hétérogènes) ▪ Optimiser le réseau par la refonte de certains éléments
Conception de logiciels sûrs	▪ Concevoir les tests du logiciel ▪ Choisir la méthodologie adaptée ▪ Participer au développement de logiciels répondant à de fortes exigences de sécurité (avionique, ferroviaire, …) : preuve de programme, analyse statique
Etude des vulnérabilités des logiciels	▪ Analyser les logiciels de type virus et Spy ware qui constituent une menace pour la sécurité des postes de travail ▪ Analyser les techniques de détournement du bon fonctionnement des logiciels ▪ Proposer des mesures préventives
Options : ▪ **Cryptographie avancée**	▪ Mettre en œuvre les outils et techniques avancées de la cryptographie
▪ **Systèmes de détection d'intrusion**	▪ Mettre en œuvre les systèmes de détection d'intrusions du marché en connaissance de leurs limites et avoir une vue prospective sur les technologies associées
▪ **Architecture N-Tiers**	▪ Mettre en œuvre des architectures N-Tiers en prenant en compte les problématiques de sécurité ▪ Connaître les principales architectures fonctionnelles pour choisir les plus adaptées
▪ **Contrôle d'accès**	▪ Maîtriser les normes et modèles de sécurité éprouvés permettant d'exprimer les politiques de sécurité adéquates à la disponibilité et à la performance du système d'information ▪ Contribuer à la disponibilité et à la performance du système d'information ▪ Analyser les modèles formels de contrôle d'accès dans le cadre du système d'information
▪ **Autour de l'authentification**	▪ Connaître et appliquer les outils de l'authentification centralisée (LDAP, Kerberos, Active Directory)
▪ **Sécurité des services en ligne**	▪ Appréhender l'ingénierie de la cryptographie pour assurer la sécurité des échanges dans les protocoles client serveur et leur authentification mutuelle

Compétences transversales

Traitement de l'information
- Produire du sens à partir de données brutes (calculs de coûts, ratios, statistiques, schémas …)
- Contextualiser l'information et la mettre en perspective
- Trier, synthétiser pour saisir un processus de travail dans sa globalité

Résolution de problème
- Traiter et résoudre des problèmes complexes
- Adopter une approche interdisciplinaire

Veille technologique
- Assurer une veille technologique sur l'évolution des systèmes de sécurité
- Etre force de proposition en matière d'amélioration des protections
- Adaptabilité et curiosité technique

Conduite de projet
- Concevoir et planifier son travail et celui de ses équipes
- Organiser, coordonner et conduire le travail au sein d'un collectif

Communiquer et rédiger en Anglais

Autres compétences transversales
- Capacités d'Analyse
- Rigueur, sens de la méthode
- Autonomie
- Réactivité
- Sens de l'écoute et des relations humaines
- Résistance au stress
- Esprit d'initiative

Débouchés

Débutants	Confirmés
▪ Responsable de parc informatique ▪ Administrateur réseau ▪ Administrateur windows ▪ Ingénieur support micro-réseau ▪ Ingénieur télécoms réseau ▪ Ingénieur réalisation sécurité ▪ Ingénieur système d'exploitation ▪ Architecte administrateur serveur ▪ Architecte réseaux ▪ Architecte infrastructures ▪ Architecte technique	▪ Auditeur systèmes d'information ▪ Consultant sécurité ▪ Consultant technique ▪ Ingénieur systèmes ▪ Ingénieur système et réseau ▪ Ingénieur maintenance, système et réseau ▪ Responsable du système d'information ▪ Directeur du service information

Environnement professionnel

- Sociétés de services en ingénierie informatique (SSII)
- Grandes entreprises privées et organisations publiques
- Éditeurs de logiciels
- PME tous secteurs d'activité

Références de stages et de travaux effectués au cours de la formation

- État de l'art sur les techniques d'établissement des clés à N. (SSII qualité logiciel)
- Mise en place d'une formation et d'une plate-forme de support pour démonstration des failles de sécurité des technologies utilisées pour la réalisation des sites Internet (SSII qualité logiciel)
- Études des outils de test de sécurité des applications web (SSII tests logiciels)
- Utilisation de Nessus (outils de test de vulnérabilité) pour réaliser des fonctions d'audit de sécurité, de détection de vulnérabilités et des tests d'intrusion sur tous équipements sur un réseau (SSII)
- Développement et mise en place d'un outils de réconciliation des @ IP LAN clients sur le réseau RAEI (Réseaux Accès Entreprises IP) (Télécom)
- Étude comparative des procédures et des méthodes d'analyse de risque portant sur la sécurité des systèmes et réseaux informatiques d'entreprises ; choix d'une méthode adaptée au contexte de l'Union des Assurances du Burkina (Université)
- Architecture centralisée de sécurité et corrélation d'événements (SSII)
- Développement d'une plateforme d'expérimentation en C permettant d'effectuer les attaques de hachage (Armement)
- Sécurité et fédération d'identité. Étude des standards de fédération d'identité, évaluation de la maturité de produits commerciaux et libres vis-à-vis de ces standards, puis maquettage pour démonstration (Aéronautique)
- Définition et étude d'architecture d'une solution de supervision des informations de sécurité sur la base de la solution eTrust Command Sécurity Center de Computer Associates (SSII)
- Analyser les fonctionnalités IAM et PKI proposées par Windows Vista (SSII)

Contacts

Responsable de la formation : Sandrine BLAZY - Professeur – Université de Rennes 1

Renseignements:
Service de Formation Continue - Université de Rennes 1 - 4, rue Kléber - 35000 Rennes - http://sfc.univ-rennes1.fr –
Tel : 02 23 23 39 50 - courriel : sfc@univ-rennes1.fr

Renseignements étudiants en formation initiale :
I.F.S.I.C. – Université de Rennes 1 - Campus de Beaulieu - 35042 Rennes Cedex - http://ifsic.univ-rennes1.fr
Tel : 02 99 84 73 92 – courriel : resp-m2-ssi@ifsic.univ-rennes1.fr