Contrat de Professionnalisation
5ème année d'ingénieur :
Informatique et Réseaux orientation Sécurité informatique

Code RNCP : 34865	Code CPF : 244185	Mise à jour : 04/05/2022

Intitulé	Durée
Bases de la sécurité	**79h** (dont 2h d'évaluation)
Sécurité du logiciel	**52h** (dont 2h d'évaluation)
Sécurité système et matérielle, rétro conception	**59h** (dont 2h d'évaluation)
Architecture réseaux et de leurs protocoles	**44h** (dont 2h d'évaluation)
Architecture réseaux sécurisés	**56h** (dont 2h d'évaluation)
Cas pratiques d'application	**35h** (dont 2h d'évaluation)
Gouvernance et Ecosystème, Conférences et Vie Privée	**64h** (dont 2h d'évaluation)
Projet de fin d'études	1h d'évaluation
Tutorat	**15h**
Sous-total enseignements (hors évaluation et tutorat)	**370 h**
Sous-total évaluations et tutorat	**30 h**
TOTAL : 400 heures *(dont 15 heures d'évaluation & 15 heures de tutorat)*	

INSA TOULOUSE & MIDISUP

INSA Toulouse Formation Continue, Batiment 7, 135 avenue de Rangueil, 31 077 Toulouse cedex 4

MIDISUP, Maison de la Recherche et de la Valorisation, 118 route de Narbonne, BP 14209 - 31432 Toulouse cedex 4

Contact : fc@insa-toulouse.fr **//** Tél : 05.67.04.88.66 // contact@midisup.com // Tél : 05.61.10.01.23

UE : Bases de la sécurité

Responsable du cours : V. Nicomette
Contenu pédagogique :
A la fin de ce module, l'étudiant devra avoir compris et pourra expliquer :

- Les principaux concepts des systèmes d'exploitation, des réseaux TCP/IP, de la programmation en langage C et en assembleur. Il s'agit ici d'une mise a niveau de tous ces domaines scientifiques, pour être sûr que les étudiants aient les bases fondamentales pour suivre l'ensemble de la formation
- Les principaux concepts de la sûreté de fonctionnement
- Les principaux concepts de la cryptographie

L'étudiant devra être capable de :

- décrire le fonctionnement des éléments importants d'un système d'information.
- décrire les principes fondamentaux de la construction des protocoles réseaux, d'analyser des traces réseaux et de comprendre l'encapsulation des flux
- utiliser les techniques de base de la programmation avec le langage C et assembleur. Il sera capable de concevoir des programmes en utilisant ces techniques.
- différencier les domaines de la sécurité (sécurity et safety) et utiliser correctement le vocabulaire associé
- distinguer les différents outils cryptographiques, comprendre ce qu'ils peuvent apporter à la sécurité et ce qu'ils ne peuvent pas
- trouver les standards internationaux de la cryptographie, comprendre leur contenu et mettre en place une utilisation d'un outil cryptographique respectant les standards ;
- réaliser des déploiements à l'aide d'outils réels de haut niveau (PKI, VPN, IPSec) ou de bas niveau (openssl) en choisissant les algorithmes, les niveaux de sécurité, les modes de fonctionnement de façon raisonnée

- Rappels et Harmonisation en architecture des ordinateurs (structure du processeur, structure des bus internes) et en système d'exploitation (processus, techniques d'ordonnancement, gestion des appels systèmes)
- Rappels et Harmonisation en réseau (l'architecure IP, le modèle OSI, protocole ARP, protocole IP, la fragmentation, les options, le protocole TCP, les protocoles du plan de gestion, RIP, BGP)
- Rappels et Harmonisation en programmation C (gestion de la mémoire, pointeurs, structures de données, entrées/sorties) et en assembleur (jeux d'instructions x86, chaînes de compilation)
- Définitions et techniques de bases de la Sécurité et Safety, éléments architecturaux, sensibilisation à la menace, techniques d'authentification, autorisation
- Cryptographie (introduction et notions de base, cryptographie symétrique, cryptographie asymétrique, standards cryptographiques et notions avancées)

Prérequis : Système d'exploitation (utilisateur), Connaissance d'un langage de programmation,
Evaluation : Examen écrit et TP

UE : Sécurité du logiciel

Responsable du cours : V. Migliore
Contenu pédagogique :
A la fin de ce module, l'étudiant devra avoir compris et pourra expliquer :

- Les différents types de vulnérabilités logicielles que l'on rencontre fréquemment, en particulier dans les programmes écrits en langage C ;
- Les contre-mesures usuelles de protections mémoires permettant de se protéger de ces différents types de vulnérabilités ;
- La théorie liée aux vers et virus, en particulier les algorithmes utilisés par les vers et virus pour infecter les systèmes informatiques et se répandre, les protections contre ces malveillances et le fonctionnement des antivirus et des méthodes qu'ils emploient
- Les bonnes pratiques pour développer du logiciel de façon sécurisée.

L'étudiant devra être capable de :

- Développer des logiciels en tenant compte des risques liés aux vulnérabilités logicielles
- Employer les méthodes formelles pour la détection de vulnérabilités logicielles ;
- Apprécier les enjeux de la protection virale, décrire les différents types d'infection informatique, analyser les techniques virales et antivirales et éagir en cas d'infection.

- Panorama des vulnérabilités logicielles : débordement dans la pile, return-into-libc, débordement dans le tas, DATA, BSS, chaînes de caractères, entiers ;
- Les risques et précautions liées à l'utilisation de programmes SUID ;
- Les contre-mesures techniques pour faire face à ces différentes vulnérabilités (les mécanismes de protection usuels des compilateurs, les canary, la randomization de l'espace d'adressage (ASLR), etc) ;
- Historique des virus et des vers ;
- Présentation des anti-virus (théorème de Cohen), des techniques de détection et de leur efficacité et de la conduite à tenir ;
- Expérimentations de techniques de détection des vers et virus ;
- Bonnes pratiques, langages restreints et cycles de développement et validation du code ;
- Programmation défensive, principes du moindre privilège dans les programmes SUID, utilisation d'API plus sûres ;
- Preuves formelles.

Prérequis : De bonnes compétences en programmation en langage C et assembleur ; Un minimum de connaissances sur le fonctionnement des OS ; Des bases en algèbre et sur l'utilisation de la théorie des automates.
Evaluation : Examens écrits et projets

UE : Sécurité système et matérielle, rétro conception

Responsable du cours : V. Migliore
Contenu pédagogique :
A la fin de ce module, l'étudiant devra avoir compris et pourra expliquer :

- Les principaux mécanismes de protection qui existent aujourd'hui dans les noyaux de systèmes d'exploitation ;
- Les principales attaques réalisées depuis le matériel ainsi que les contre-mesures associées ;
- Le fonctionnement des principaux composants matériels pour la sécurité tels que les hyperviseur et les IOMMU ;
- L'intérêt des dernières avancées en terme de protection matérielle réalisées par les fondeurs de processeurs et de chipset ;
- Le fonctionnement des attaques matériels et physiques principales qui ciblent les systèmes informatiques ;
- La rétro-conception de logiciels (reverse engineering) tout en étant capable d'expliquer la la chaîne de compilation avec les modèles utilisés par les compilateurs pour générer le code machine ;
- Les stratégies pour rendre la rétro-conception de logiciels plus difficile à réaliser.

L'étudiant devra être capable de :

- Identifier les composants logiciels les plus adaptés pour protéger un système d'exploitation vis-à-vis des attaques logicielles ;
- Identifier les menaces provenant des couches basses et les vecteurs d'attaques à considérer dans un système ;
- D'obtenir une vue globale des échanges entre les composants matériels d'un système pour identifier les composants critiques et déterminer les contre-mesures a intégrer dans le système d'exploitation ;
- Identifier les menaces sur les composants physiques d'un système ;
- De réaliser une rétro-conception de maliciels pour en comprendre le fonctionnement voire créer des signatures pour les détecter.

Etudes des noyaux Linux et Windows du point de vue de la sécurité :

- Mécanismes noyau de protection de l'espace utilisateur
- Attaques sur le noyau depuis l'espace utilisateur (via abus de privileges, ...)
- Protection du noyau face à des attaques depuis l'espace utilisateur
- Ouverture sur la protection du noyau face aux attaques de composants matériels

Composants matériels des systèmes d'information pour la sécurité :

- Panorama des composants matériels présents dans un système informatique
- Utilisation de ces composants pour améliorer la sécurité (virtualisation, TPM, IO-MMU)
- Création d'une chaîne de confiance au démarrage basée sur l'utilisation de matériels de confiance
- Présentation de projets de recherche utilisant le matériel comme support pour la sécurité
- Mise en pratique de ces concepts par le développement d'une solution de sécurité sur architecture Intel

Attaques et sécurisations matérielles :

- Rappels fondamentaux de microélectronique et d'architecture matérielle
- Canaux auxiliaires (SPA, DPA, ...)
- Contre mesures matérielles et algorithmiques

- Démonstration d'une attaque Bellcore sur un processeur grand public

Chaîne de compilation
- Introduction aux techniques de compilation
- Analyse de graphes de controles et de donnees

Techniques de rétro conception logicielle
- Introduction à la rétro-ingénierie: méthodologie et outils
- Découverte et prise en main des outils: désassembleurs, débuggers et de leurs languages de scripting
- Application à l'analyse de code malveillant et/ou à l'exploitation de vulnérabilité
- Initiation à l'outil IDA

Prérequis : De bonnes compétences en programmation en langage C et assembleur ; Un minimum de connaissances sur le fonctionnement des OS ; Des bases en algèbre et sur l'utilisation de la théorie des automates.
Evaluation : Examens écrits et projets

UE : Architecture réseaux et de leurs protocoles

Responsable du cours : V. Nicomette
Contenu pédagogique :
A la fin de ce module, l'étudiant devra avoir compris et pourra expliquer :
- Les principaux concepts de la sécurité des réseaux filaires, les principales attaques ciblant ces réseaux et les mécanismes de protection associés
- Les principaux concepts de la sécurité des réseaux non filaires (Wifi, GSM, GPRS, LTE, UMTS)
- Les principales faiblesses des protocoles réseaux fragiles et comment les sécuriser.

L'étudiant devra être capable de :
- Reconnaître et mettre en place les attaques réseau classiques dans le cadre d'un test d'intrusion ; identifier et mettre en place les mécanismes de protection contre ces attaques ; utiliser et mettre en place des infrastructures de defense
- Choisir une solution de sécurité adaptée pour un pointenti d'accès Wifi ; réaliser un test d'intrusion sur un point d'accès Wifi
- Différentier les objectifs de sécurité dans les différents réseaux cellulaires ; décrire les mécanismes d'authentification et d'échange de clés et comparer les apports en sécurité de chacun ; décrire les attaques possibles dans le cadre de chaque technologie ; reconnaître les éléments architecturaux de la sécurité dans un réseau d'opérateurs
- Reconnaître les protocoles fragiles mis en place habituellement dans un réseau informatique ; sécuriser ces protocoles fragiles par l'utilisation de tunnels pour les applications lorsque ceci est nécessaire ; utiliser SSH et les fonctions associées (transfers de fichiers, proxys, etc.) ; décrire les bonnes pratiques pour la définition d'un protocole sécurisé

Prérequis : De bonnes compétences dans l'informatique en général et dans la compréhension des protocoles réseaux qui régissent l'Internet (TCP/IP, protocoles de routage a minima). En particulier, toute la terminologie doit être connue et les principes fondamentaux de la cryptographie doivent être acquis
Evaluation : Examens écrits

UE : Architecture réseaux sécurisés

Responsable du cours : V. Nicomette
Contenu pédagogique :
A la fin de ce module, l'étudiant devra avoir compris et pourra expliquer :

- Les principaux concepts associés à la conception et l'implémentation d'architectures réseaux sécurisées
- Les outils et techniques principaux permettant cette sécurisation et leur utilisation en fonction des différents contextes ainsi que des objectifs correspondants.

L'étudiant devra être capable de :

- Distinguer les différents types de pare-feux ainsi que leurs capacités et limitations
- Définir et auditer une architecture de filtrage adaptée à un réseau informatique donné
- Choisir pour un tunnel IPsec les protocoles à utiliser, les modes de fonctionnement et un plan de routage adapté pour les passerelles associées
- Mettre en place et auditer un tel tunnel Ipsec
- Mettre en place ou auditer un VPN créé sur du IPsec manuellement ou en utilisant les outils tout-en-un du marché
- Mettre en place et auditer un système de détection d'intrusion éventuellement distribué avec des options de prévention
- Faire le design complet d'une architecture de sécurité pour un réseau complexe

Evaluation : Examen écrit et TP

UE : Cas pratiques d'application

Responsable du cours : E. Alata
Contenu pédagogique :
A la fin de ce module, l'étudiant devra avoir compris et pourra expliquer :

- Les différentes techniques utilisées de nos jours pour sécuriser les communications sol/air dans le contexte satellitaire ;
- Les problématiques liées aux différents types de mission et les standards utilisés ;
- Les moyens pour la sécurisation des transmissions par étalement de spectre (TRANSSEC) ;
- Les principes du réseau informatique pour la gestion du trafic aérien (ATM) et les problématiques de sécurité associées ;
- Lister et quantifier les vulnérabilités inhérentes aux architectures système et réseau et les grandes techniques d'intrusion ;
- Expliquer le fonctionnement des principales vulnérabilités du web.

L'étudiant devra être capable de :

- Effectuer des choix pertinents vis-à-vis de la sécurité pour architecturer les moyens de communication sol/air ;
- Identifier les limites et avantages de différentes solutions de détection d'intrusion ;
- Positionner les sondes de détection d'intrusion de manière efficace ;
- Analyse les évènements collectés par les sondes et corréler ces évènements pour identifier une menace réelle.
- Identifier les vulnérabilités dans les architectures web et proposer des solutions pour réaliser une protection efficace.

Sécurisation des communications satellitaires (chiffrement, authentification, TRANSSEC)
Architecture ATM et protocoles sécurisés pour les communications aéronautiques (12h)

- Introduction du concept de réseau industriel
- Limites sécuritaire des réseaux industriels actuels
- Complexité du réseau ATM actuel
- Détection d'intrusion pour les réseaux ATM actuels
- Gestion security vs safety dans l'ATM

Sécurité des Applications Web

- Présentation des attaques et vulnérabilités sur le web
- Mécanismes de défense côté navigateur et serveur
- Présentation de projets de recherche sur la détection
- Mise en pratique des attaques et des protections

Cartographie/découverte
Techniques d'intrusion réseau et système

- Stratégies d'intrusion (recueil d'informations, exploitation de vulnérabilités, pivot, cryptanalyse, reverse engineering)
- Les outils d'intrusion (Nmap, Metasploit, Craqueurs de mots de passe, pivots ssh, proxychains, debugger, compilateur)

Analyse forensics

- Traitement des incidents, continuité, investigation- numérique

Prérequis : De bonnes connaissances des architectures web ; Des bases en cryptographie ; Des bases en réseaux.
Evaluation : Examens écrits et projets

UE : Gouvernance et Ecosystème, Conférences et Vie Privée

Responsable du cours :
Contenu pédagogique :
Gouvernance de la sécurité
Ce cours présente divers aspects de la sécurité dans le monde de l'entreprise avec un intérêt particulier pour les questions locales, humaines et organisationnelles.

A la fin de ce cours l'étudiant saura :

- Identifier les principaux éléments juridiques liés à la SSI
- Reconnaître et définir les principaux acteurs chargés de la sécurité à l'intérieur et autour d'une entreprise, ainsi que les difficultés associées.
- Identifier les enjeux et les parties prenantes, au sien d'une organisation, pour définir et élaborer les briques de base d'une démarche de gouvernance de la sécurité.
- Apprécier les besoins en sécurisation à satisfaire et les objectifs de sécurité à atteindre pour mettre en place des exigences de sécurité d'ordres juridique / organisation / technique, aux niveaux des mesures de prévention / protection / récupération.
- Structurer et organiser les catégories de risques-types existant en matière de sécurité et caractériser et apprécier l'efficacité de modes et mesures de traitement des risques (réduction/augmentation, évitement/rejet, partage/transfert, maintien/acceptation).
- Appliquer les concepts des politiques de sécurité et des différents documents associés dans une entreprise ou dans les cadres réglementaires usuels (PSSI E, guides officiels, etc …)
- Manipuler et ordonner les principaux modèles de sécurité formels associés aux systèmes logiciels des plus hauts niveaux de sécurité ; et apprécier les propriétés de sécurité associées.
- Identifier et caractériser les principales techniques d'évaluation de la sécurité (les approches qualitatives industrielles et certains travaux de recherche).
- Apprécier comment défendre un système d'information orienté système industriel comme celui de la navigation Aérienne, contre des intentions potentiellement hostiles utilisant les systèmes de traitement de données.
- Apprécier et appliquer les concepts régissant une politique de sécurité spécifique à la problématique des systèmes d'information hybrides (industriels).

Ecosystème de la sécurité

Cette matière est composée d'un ensemble de conférences permettant aux étudiants 1) de découvrir les principaux acteurs composant l'écosystème de la sécurité et 2) d'approfondir certains aspects de la sécurité informatique.

Concernant les principaux acteurs composant l'écosystème de la sécurité, différentes interventions sont programmées, par un représentant de l'ANSSI, un représentant du CERT-IST, le FSD (Fonctionnaire Sécurité Défense) de l'INSA notamment. Par ailleurs, certaines thématiques importantes de la sécurité sont ici approfondies, comme la sécurité dans le milieu médical, le milieu bancaire. Ces thématiques peuvent varier en fonction des années.

Conférences et Vie Privée

Des conférences sur la sécurité permettent aux étudiants de découvrir des facettes particulières de la sécurité au travers de brèves interventions. Chaque conférence fait l'objet d'un ou de 2 créneaux de cours au maximum. Le contenu de ces conférences peut varier en fonction des années, puisque nous souhaitons proposer aux étudiants des thématiques importantes qui sont au cœur de l'actualité scientifique de la sécurité informatique. Par exemple, certaines conférences sont liées à des métiers spécifiques de la sécurité et à ce titre des interventions sont faites par la Marine Nationale, la DGSI, par le CERT Eurocontrol. D'autres conférences permettent de découvrir des aspects importants de la sécurité, comme la protection de la vie privée (et notamment la RGPD), la présentation des aspects juridiques relatifs à la sécurité ou la présentation des principaux OIV et des problématiques de la sécurité qui leur sont relatives.

UE : Projet de fin d'études

Responsable du cours : Directeur du département d'ingénierie et tuteur pédagogique
Contenu pédagogique :
L'étudiant devra être capable de :

- Mettre en application les connaissances théoriques acquises
- Mettre en œuvre son initiative individuelle au profit d'une réalisation concrète au sein de l'entreprise
- Pratiquer la prise de responsabilité et la gestion de projet

Prérequis : validation pédagogique de la fiche missions de l'alternant
Evaluation : rapport écrit et soutenance orale