MASTÈRE SPÉCIALISÉ SÉCURITÉ INFORMATIQUE

RÉSUMÉ DE LA FORMATION

Type de diplôme : Mastère spécialisé
Domaine ministériel : Sciences, Ingénierie et Technologies

ETABLISSEMENTS COACCRÉDITÉS

* ENAC Toulouse
* Institut National des Sciences Appliquées de Toulouse

PLUS D'INFOS

Niveau d'étude : BAC +6

Public concerné
* Formation continue
* Formation initiale

Nature de la formation : Diplôme

EN SAVOIR PLUS

http://www.enseeiht.fr/fr/index.html

Organisation de la formation

Mastère Sécurité informatique

Composante

École Nationale Supérieure d'Électrotechnique d'Électronique d'Informatique d'Hydraulique et des Télécommunications

Lieu(x) de la formation

Toulouse

Contact(s) administratif(s)

n7@enseeiht.fr

Mastère Sécurité informatique

PLUS D'INFOS

Organisation de la formation

· Année Mastère SI

· Semestre 10-Mastère SI

· UE STAGE/THESE PROFESSIONNELLE

Responsable(s)
AGUILAR MELCHOR CARLOS

· Semestre 9-Mastère SI

· UE Sécurité du logiciel

· Matière Vulnérabilités logicielles

Objectifs

Apprentissage des concepts suivants :

* Vulnérabilités logicielles diverses
  * BOF diverses (piles, tas, BSS)
  * chaînes de format
  * integer overflow
  * programme SUID
  * return oriented programming
* Analyse statique undefined behavior
* Contre-mesures (Control Flow integrity, etc.)
* OpenBSD

Description

L'objectif de ce cours est de présenter aux étudiants différents types de vulnérabilités logicielles que l'on rencontre fréquemment, en particulier dans les programmes écrits en langage C, langage qui sera le support pour ce cours. Les contre-mesures usuelles protections mémoires permettant de se protéger de ce type de vulnérabilités sont également proposées.

A l'issue de cet enseignement, l'étudiant saura analyser un programme et juger de son niveau de sécurité en considérant les vulnérabilités logicielles présentées dans cet enseignement. Il sera capable d'identifier les tests à réaliser pour mettre en évidence l'existence d'une vulnérabilité logicielle. Il sera également capable de comparer différentes contre-mesures, d'identifier le plus adapté pour corriger une vulnérabilité et de le mettre en œuvre.

Enfin, on expose les bonnes pratiques de développement pour la sécurité. À l'aide du cas d'étude OpenBSD, les étudiants apprennent par exemple les bon choix architecturaux et fonctions de la bibliothèque standard C à utiliser ou éviter.

· Matière Virus et techniques virales

Objectifs

Apprentissage des concepts suivants :

* Présentation des virus et vers
* Présentation des anti-virus
* Expérimentations

Description

L'objectif de ce cours est de présenter aux étudiants la théorie liée aux vers et virus. Une première partie est consacrée à l'étude des algorithmes utilisés par les vers et virus pour infecter les systèmes informatique et se répandre. Cette connaissance est nécessaire pour appréhender les protections conctre ces malveillances. Ces protections font l'objet de la seconde partie qui se consacre plus particulièrement sur les anti-virus avec les méthodes qu'ils utilisent pour la détection des vers et virus. A l'issue de ce cours, l'étudiant saura apprécier les enjeux de la protection virale, décrire les différents types d'infection informatique, analyser les techniques virales et antivirales et réagir en cas d'infection.

· Matière Développement logiciel sécurisé

Objectifs

Apprentissage des concepts suivants :

* Analyse Statique
* Preuves formelles pour conception de systèmes sécurisés par construction

Description

L'objectif de ce cours est de présenter un ensemble de bonnes pratiques pour développer du logiciel de façon sécurisée. Ces bonnes pratiques sont illustrées avec le système OpenBSD qui est reconnu pour avoir adopté des méthodes de développement rigoureuses. Une présentation des méthodes formelles pour la détection de vulnérabilités sera également

réalisée.

A l'issue de cet enseignement, l'étudiant doit être capable de comprendre les enjeux du développement logiciel sécurisé, en connaître les principales méthodes et être capable de proposer l'utilisation de ces méthodes en fonction du logiciel qui est développé, de sa

fonction et du contexte dans lequel il est utilisé.

· UE GOUVERNANCE ET ECOSYSTEME DE LA SECURITE

· Matière Gouvernance de la sécurité

Objectifs

Apprentissage des aspects :

* Gouvernance
* Critères communs

* Politiques de sécurité
* Évaluation de la sécurité

Description

Cette série de conférences présentera divers aspects de la sécurité dans le monde de l'entreprise avec un intérêt particulier pour les question légales, humaines et organisationnelles.

A la fin du 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 sein 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 des modes et mesures de traitement des risques (réduction / augmentation, évitement / rejet, partage / transfert, maintien / acceptation).
* Apprécier et appliquer les concepts régissant une politique de sécurité spécifique à des secteurs d'activité de sensibilité particulière (santé, social, médical, sociétal) et/ou nécessitant de satisfaire des enjeux élevés en matière de continuité d'activité.
* Appliquer les concepts des politiques de sécurité et les 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 certaines 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)

· Matière Ecosystème de la sécurité

Objectifs

Apprentissage des aspects suivants :

* Écosystème de la cybersecurité : services de l'état (ANSSI), CESTIs, CSPNs, CERT-IST, etc.
* Expertise Judiciaire et Audit
* Sécurité et santé
* Sécurité dans le bancaire
* Gendarmerie
* Fonctionnaires sécurité / défence

Description

Conférences diverses dispensées majoritairement par des intervenants extérieurs du métier de la sécurité.

· UE FONDAMENTAUX DE LA SECURITE

· Matière Rappels et Harmonisation en systèmes d'exploitation

Objectifs

Rappels concernant :

* Architecture matérielles
* Système d'exploitation

Description

L'objectif de ce cours est de mettre l'ensemble des étudiants à niveau sur les principaux concepts fondamentaux des systèmes informatiques, en particulier ceux qui sont utiles pour les différents enseignements de sécurité par la suite. Les principaux points abordés concernent les architectures matérielles des ordinateurs, les concepts fondamentaux des systèmes opératoires (espace noyau, espace utilisateur, processus et les mécanismes d'ordonnancement associés, etc).
A l'issue de cet enseignement, l'étudiant sera capable de décrire le fonctionnement des éléments importants d'un système d'information. Sur cette base, il sera capable d'analyser ces éléments pour déterminer leur impact sur la sécurité du système.

· Matière Rappels et Harmonisation en réseau

Objectifs

Rappels concernant :

* Le modèle OSI
* Potocoles du plan de gestion, protocoles de routage

Description

L'objectif de ce cours est de mettre l'ensemble des étudiants à niveau sur les principaux concepts fondamentaux des réseaux d'ordinateurs, en se focalisant sur les concepts des réseaux IP.
Les principaux points abordés concernent les couches MAC, réseaux et transports (tels que DHCP, ARP, IP ou TCP), mais également certains protocoles applicatifs particulièrement sensibles du plan de gestion (tels que les protocoles d'annuaires avec le DNS ou le routage avec RIP ou BGP).
A l'issue de cet enseignement, l'étudiant sera capable de décrire les principes fondamentaux de la constructions des protocoles réseaux, sera capable d'analyser des traces réseaux et sera en mesure de comprendre l'encapsulation des flux. Il sera en mesure de proposer l'utilisation de certains protocoles et services en fonction des besoins. En particulier, il sera en mesure de comprendre les principaux éléments des protocoles réseaux qui peuvent avoir des impacts sur la sécurité.

· Matière Rappels et Harmonisation en programmation C et assembleur

Objectifs

Rappels concernant :

* Le language C pointeurs, structures. Approfondissements de concepts avancés tels que les sections mémoire, etc.
* Assembleur *inline*

Description

L'objectif de ce cours est de mettre l'ensemble des étudiants à niveau sur les principaux concepts fondamentaux de la programmation. Les langages orientés bas-niveaux seront privilégiés car ce sont ceux qui

seront le plus abordés lors de l'analyse de problèmes de sécurité. Les langages abordés seront donc le

langage C et l'assembleur, en particulier sur architecture x86.

A l'issue de ce cours, l'étudiant maîtrisera les techniques de base de la programmation avec le langage C et

assembleur. Il sera capable de concevoir des programmes en utilisant ces techniques. Il sera capable

d'analyser précisément un programme écrit avec ces langages pour en comprendre son fonctionnement. Il sera

également capable de comprendre le fonctionnement de programmes écrits dans des langages différents.

· Matière Définitions et Techniques de base de la sécurité et Safety

Objectifs

Introduction et définition des points suivants :

* Définitions principales (AAA, CID, politiques de sécurité, évaluations)
* Types d'attaques / classification
* Sensibilisation (menaces, grandes attaques historiques)
* Tolérance aux fautes et Sûreté de Fonctionnement (1CM)

Description

Ce cours présentera la terminologie et les bases fondamentales de la sécurité et de la tolérance aux fautes.

A l'issue de ce cours, l'étudiant saura :

* différencier les domaines de la sécurité (security et safety)
* distinguer et utiliser correctement les termes correspondant : aux propriétés de sécurité de l'information et des systèmes ; et aux techniques apportant la sécurité
* appréhender la sécurité dans sa globalité en allant au-delà des questions techniques et en prenant en compte les aspects organisationnels
* modéliser les différents types d'attaquant
* reconnaître les grands outils et éléments architecturaux apportant de la sécurité dans un réseau comme dans un système
* décrire les différentes approches pour authentifier un utilisateur et autoriser des actions sur un système informatique

· UE CRYPTOGRAPHIE

Responsable(s)
AGUILAR MELCHOR CARLOS

· Matière Cryptographie

Objectifs

Apprentissage et maîtrise des aspects suivant de la cryptologie :

* Cryptographie (primitives sans clé, à clé symétrique et asymétrique)
* Cryptanalyse (attaques cryptographiques)
* Cryptographie appliquée (protocoles réseau, enclaves de sécurité, preuve de protocoles, etc.)

Description

Ce cours présente dans un premier temps les bases de la complexité pour la cryptographie et la notion d'aléa. Ensuite la cryptographie symétrique et asymétrique ainsi que les attaques habituelles sont décrites. Enfin les standards modernes et quelques notions de cryptographie avancée sont introduits. Tout ce cours alternera l'introduction aux techniques cryptographique et définitions de sécurité et notions d'attaque (qui n'ont un sens que face à des techniques cryptographiques).

A l'issue de ce cours, l'étudiant saura :

* distinguer les différents outils cryptographiques, comprendre ce qu'ils peuvent apporter à la sécurité et ce qu'ils ne peuvent pas appliquer les bonnes pratiques, et comprendre les dangers d'une utilisation inappropriée ;
* utiliser les termes techniques de la cryptographie et rechercher les propriétés qui peuvent apporter des contributions à des problèmes complexes de sécurité ;
* trouver les standards internationaux de la cryptographie, comprendre leur contenu et mettre en place une utilisation d'un outil cryptographique respectant les standards ;
* identifier les dangers classiques (homme du milieu, attaques par canaux cachés) et utiliser des modèles d'attaquant larges pour définir si une nouvelle utilisation d'un outil cryptographique est sûre ou pas

· UE Sécurité du Matériel., Rétro Conception

· Matière Protection des systèmes d'exploitation

Objectifs

Apprentissage des aspects suivants :

* Sécurité des systèmes d'exploitation
* Le cas GNU / Linux
* Le cas Windows

Description

L'objectif de ce cours est de présenter les principaux mécanismes de protection qui existant aujourd'hui dans les noyaux de systèmes d'exploitation. Ce cours aborde également un certain nombre d'attaques permettant d'exploiter des vulnérabilités des noyaux de système eux-mêmes. Il se base sur les noyaux de système Linux et Windows. Il fournit également un panorama des outils et techniques disponibles pour protéger les données contenues dans les systèmes de fichiers et dans la mémoire. La plupart de ces techniques reposent sur des méthodes de chiffrement et sur des contrôles d'accès.

A l'issue de ce cours, l'étudiant devra être capable d'identifier les propriétés de sécurité à préserver concernant les données manipulées dans un système pour ainsi déterminer de les protections les plus adaptées à mettre en œuvre. L'étudiant sera également capable d'analyser un système d'exploitation pour identifier les menaces et les vulnérabilités qui peuvent l'affecter. Il sera capable de décrire les conséquences liées à l'exploitation de ces vulnérabilités. Il sera capable d'exposer les différents mécanismes de protection pour contenir ces menaces. Il sera capable de choisir et d'implémenter le mécanisme le plus adapté au système en train d'être étudié.

· Matière Attaques matérielles, composants matériels pour la sécurité

Objectifs

Apprentissage des aspects suivants :

* Composants matériels pour la sécurité (virtualisation, IO-MMU, TPM)
* Attaques matérielles (canaux auxiliaires) et contre-mesures
* Classes d'attaques Spectre, Meltdown, rowhammer et canaux auxiliaires temporels à l'aide des caches

Description

L'objectif de ce cours est de présenter les principales attaques réalisées depuis le matériel ainsi que les contre-mesures associées. Un balayage des composants d'un système sera réalisé en identifiant l'utilité et les risques associés à la présence de chacun de ces composants. Certains de ces risques seront illustrés par des attaques récentes, soit en reconfigurant les composants concernés, soit en réalisant une étude matérielle et physique de ces composants. Aussi, des contre-mesures seront présentées avec les dernières avancées en terme de protection matérielle réalisées par les fondeurs de processeurs et de chipset.

A l'issue de ce cours, l'étudiant devra être capable d'obtenir une vue globale des échanges entre les composants matériels d'un système d'information, en considérant aussi bien les composants logiciels et réseaux que matériels. Il sera capable de comprendre le fonctionnement d'une attaque sur le matériel, de la décrire et d'expliquer les mécanismes de

protection associés. Il sera également capable d'identifier les composants critiques d'un système, d'analyser les vulnérabilités pouvant cibler ces composants, de déterminer les contre-mesures permettant de les protéger et de mettre en œuvre ces contre-mesures.

· Matière Reverse engineering

Objectifs

Apprentissage des aspects suivants :

* Chaîne de compilation
* Techniques de retro-conception logicielle

Description

L'objectif de ce cours est de présenter aux étudiants les activités autour de la rétro-conception de logiciels (reverse engineering). Dans un premier temps, la chaîne de compilation est présentée avec les modèles utilisés par les compilateurs pour générer le code machine. Dans un second temps, des stratégies sont présentées pour inverser ce processus pour premettre de mieux comprendre certaines parties d'un code logiciel. Pour finir, les contre-mesures à la rétro-conception sont présentées pour rendre cette activités plus difficile.

A l'issue de cet enseignement, l'étudiant sera capable d'analyser précisément et de décrire globalement le fonctionnement d'un programme en se basant uniquement sur le code assembleur. Il sera capable d'appliquer les acquis des enseignements liés à l'étude des vulnérabilités pour identifier des vulnérabilités dans ces programmes. Il sera capable de justifier l'existence des vulnérabilités en mettant en œuvre une preuve de concept de l'exploitation.

· UE SECURITE DES RESEAUX

Responsable(s)
AGUILAR MELCHOR CARLOS

· Matière Attaques et sécurisation des couches OSI

Objectifs

Apprentissage des aspects suivants :

* Couches 1-5 (Principe, Attaques, Défense)
* Couche 7 (illustration avec DNS et BGP)
* Dénis de service
  * Métrologie
  * botnets et Dénis de service distribué

Description

Ce cours présente les principales attaques et contre-mesures sur les couches OSI en commençant par les attaques sur le lien physique et en allant vers les attaques applicatives sur les protocoles indispensables au bon fonctionnement d'un réseau. À la fin de ce cours l'étudiant saura :

* 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
* Informer sur les dangers inhérents à un réseau informatique et connaître les limites des protections que l'on peut obtenir à un coût raisonnable
* Informer sur les apports des grandes infrastructures de sécurité DNS, et BGP mises en place par l'ICANN

Utiliser et mettre en place ces infrastructures.

· Matière Sécurité des réseaux non filaires

Objectifs

Apprentissage des aspects suivants :

* Protection des réseaux Wifi (portail captifs + WPA + 802.1X + EAP)
* Sécurité réseaux cellulaires (GSM/GPRS/UMTS/LTE)

Description

Cet enseignement présente la sécurisation des réseaux cellulaires de GSM à 5G ainsi que les attaques et la sécurisation des réseaux WiFi.

À la fin de ce cours l'étudiant saura dans le domaine du WiFi :

* Choisir une solution de sécurité adaptée pour un point d'accès
* Comprendre et choisir les multiples options disponibles pour chaque solution
* Mettre en avant les apports en sécurité et limites de la solution choisie
* Réaliser un test d'intrusion sur un point d'accès

À la fin de ce cours l'étudiant saura dans le domaine des réseaux cellulaires :

* 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 technologies
* Reconnaître les éléments architecturaux de la sécurité dans un réseau d'opérateurs

· Matière Sécurisation des protocoles

Objectifs

Apprentissage des aspects suivants :

* Protocoles fragiles
* Sécurisation a priori
* Sécurisation a posteriori (ex. tunnels SSH)

Description

Ce cours met en avant les nombreux protocoles fragiles utilisés de nos jours et décrit les bonnes pratiques pour concevoir des protocoles sûr a posteriori et des techniques pour sécuriser des protocoles fragiles a posteriori par l'utilisation de tunnels.

À la fin de ce cours l'étudiant saura :

* Reconnaître les protocoles fragiles mis en place habituellement dans un réseau informatique
* Sécuriser les protocoles fragiles par l'utilisation de tunnels pour les applications où ceci sera nécessaire
* Utiliser SSH et les fonctions associées (transfers de fichiers, proxys, etc.)
* Décrire les bonnes pratiques pour la définition d'un protocole sécurisé

· Matière Composants fondamentaux d'une architecture sécurisée

Objectifs

Apprentissage des aspects suivants :

* Firewalls
* IPSEC et VPN
* NIDS (Sondes, SIEM, etc.)
* IAM Cours et TD

Description

Cet cours présente les éléments architecturaux indispensables à la sécurisation d'un réseau : Firewalls, NIDS, IPsec, VPN et outils de gestion des identités.

À la fin de ce cours l'étudiant saura :

* 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
* Faire le design complet d'une architecture de sécurité pour un réseau complexe incluant la gestion des identités et de l'authentification

· UE BUREAU D'ETUDES ET CHALLENGES

Responsable(s)
AGUILAR MELCHOR CARLOS

· Matière Bureau d'étude ARS

Objectifs

Apprentissage des aspects suivants :

* Amélioration d'une archi de sécurité et mise en place d'un système de logs et SIEM
* BE ASA Cisco (VPN + Firewall + IDS)
* Vulnérabilités Web

Description

Ce bureau d'étude a pour but de mettre en pratique les divers enseignements du module réseau.

À la fin de ce cours l'étudiant saura :

* 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
* Mettre en place une architecture de logs avec un système centralisé de gestion des événements

· Matière Intrusion système et réseaux

Objectifs

Apprentissage des aspects suivants :

* Challenge réseaux
* Analyse Forensics

Description

Tout d'abord le cours présentera un panorama des attaques qui exploitent les technologies employées pour la conception de sites web et fournit des éléments pour protéger ces systèmes. Le cours se poursuivra en présentant aux étudiants les risques auxquels ils devront faire face et en leur faisant réaliser que le comportement d'utilisateurs légitimes peut être exploité par des attaquants pour cibler les systèmes.

Ensuite, l'étudiant sera confronté à plusieurs challenges, qui lui permettront concrètement de se placer dans la peau d'un attaquant et d'exploiter des vulnérabilités de différentes natures : 1) un premier challenge illustrant les techniques d'intrusion dans un réseau ; 2) un second challenge centré sur la mise en oeuvre des techniques d'intrusions et d'élévation de privilèges sur un système informatique ; et 3) un cours/TP traitant de la réaction en cas d'incident avec une mise en pratique de techniques d'investigation numérique sur un système, après intrusion.

A l'issue de ce cours l'étudiant saura lister et quantifier les vulnérabilités inhérentes aux architectures système et réseau et sera sensibilisé aux grandes techniques d'intrusion

· UE SECURITE DANS L'AERONOTIQUE

· Matière Gouvernance aéro-spacial

· Matière Architecture ATM et protocole séc. pour les com° aéronaut.

· Matière Cas d'Airbus

· Matière Cas de la DRAC

· Matière Aspects juridiques

· Matière PSSI dans le Contrôle Aérien

· Matière Sécurisation des Communications Satéllitaires

· UE APPROFONDISSEMENTS

· Matière Droit du numérique

· Matière Sécurité et Psychologie Sociale

· Matière IPMA

· Matière Virtualisation

· Matière IAM

· UE CONFERENCES

· Matière Conférences (vie privée)

Objectifs

Apprentissage des aspects suivants :

* Management de la vie privée
* Aspects juridiques
* Geoprivacy
* Sécurité physique dans les aéroports
* Sécurité physique pour un constructeur aéronautique
* Ingénierie sociale
* Loi de Programmation Militaire, protection des Opérateurs d'Importance Vitale (OIV)

Description

Ce cours présentera les bases légales, les enjeux, et les principaux outils de la protection de la vie privée. Plus précisément, l'objectif de ce cours est :

* De présenter les enjeux de la protection de la vie privée dans les systèmes d'information
* De caractériser l'ensemble de la problématique liée à la protection des données à caractère personnel
* D'illustrer cette problématique dans certains cas particuliers assez sensibles, en faisant la distinction entre Security et Privacy, et aussi entre RSSI et CIL (futur DPO), ou encore entre une analyse de risques en SSI et analyse d'impact sur le respect de la vie privée (ou Privacy Impact Analysis)
* De matérialiser certaines solutions techniques déployées dans certains domaines d'activité bien spécifiques, à travers les techniques d'anonymisation et/ou de pseudonymisation (par exemple : ré-utilisation de données de santé anonymisées, ou de géolocalisation)
* De décrire les techniques d'attaque contre l'anonymisation
* De présenter les principaux outils techniques de la protection de la vie privée.

Composante

École Nationale Supérieure d'Électrotechnique d'Électronique d'Informatique d'Hydraulique et des Télécommunications